School internet use: case studies in the sociology of risk

Hope, Andrew Derek

Andrew Derek Hope

School Internet Use: Case Studies in the Sociology of Risk

Degree of Doctor of Philosophy in Education

Thesis submitted: 2002

Abstract

This research uses observation, interviews and content analysis to examine the perceived and actual risks arising from Internet use in eight educational establishments. The majority of staff interviewed expressed concern about on-line pornography and the dangers of web based chat rooms. Additionally staff were anxious about the risks posed by hate engendering sites, websites encouraging experimentation, copyright infringement and threats to network security. In considering these school Internet risk narratives I make a distinction between concern that the student is "at risk" and that they are "dangerous", posing a threat to the institution. I point out that in the primary schools staff talked about students solely as being "at risk", whereas in secondary schools this concern was tempered with the view that students misusing the school Internet also posed a danger to the institution. In the post-16 college Internet risks were almost solely expressed in terms of the "dangerous student". While only a sparse student risk narrative existed, with a few students anxious about on-line pornography, chat-lines and security there was non-verbal evidence indicating that students were worried about being punished for misusing the Internet. In assessing the "student- at-risk", I argue that exposure to pornography via the school Internet was not likely to pose an actual risk, while undesirable others in chat rooms, hateful websites and sites encouraging experimentation all posed actual, though statistically remote, risks. Considering the Internet activities of the "dangerous student", I found little evidence to suggest that the issues of school image, staff authority and copyright should be a source of great concern, although I note that school network security was an actual risk which deserves more attention. Finally, I consider institutional attempts to control Internet use and alleviate some of these perceived and actual risks through the use of rhetoric, exclusion and surveillance.

School Internet Use: Case Studies in the Sociology of Risk

Andrew Derek Hope

Degree of Doctor of Philosophy in Education

University of Durham

School of Education

Thesis submitted: 2002

Statements of Protocol

None of the material submitted in this thesis has previously been submitted for a degree in this or any other university.

To ensure anonymity the names of staff, students and the eight educational institutions involved in the research have been changed.

This thesis conforms with the word limit set out in the Degree Regulations for the University of Durham.

Word count: 99, 699

Table of contents

List of Tables

Overview

This research focuses on the perceived and actual risks arising from Internet use in eight educational institutions. Chapters one, two and three provide details of the rationale, relevant literature, research background and methods. Chapters four, five and six focus upon the staff / student perceptions of risks arising from school Internet use. Chapters seven and eight make an assessment as to whether the risks described by staff and students are perceived or actual. Finally chapters nine, ten and eleven examine institutional attempts to control Internet use through the use of rhetoric, exclusion and surveillance. Throughout this research two main issues emerged, namely the identification of students as being at risk and / or a source of danger and the differential labelling of particular age groups. I will now provide an overview of each chapter in turn.

In the first three chapters I provide a background to my research into the risks arising from Internet use in schools. In chapter one I consider the rationale for this research into school Internet risks, arguing that five questions need to be addressed. These are (1) why study the social impact of the Internet (2) why situate the study of Internet use in schools (3) why use the concept of risk (4) why associate risk with schools and (5) why, in particular, focus upon risks arising from school Internet use? Answering these questions I observe that the Internet is a novel, rapidly growing technology, that the government is seeking to connect all of Britain's schools to the "web" through the National Grid for Learning (NGfL) initiative, that risk is a topic recently focused upon by academics, which provides a useful conceptual framework and that following certain high profile incidents, such as Dunblane, schools have become identified as risk environments. Finally I explain that this focus emerged partially from the research, which in turn drew my attention to the wider Internet risk narratives evident in the mass media, government documentation and special interest group publications.

In chapter two I review the literature on the social impact of the Internet and the sociology of risk. As there is a lack of literature focusing on Internet "risks" I consider the subjects of the Internet and risk separately before drawing together

some common threads. Exploring the existing social research about the Internet, under the headings of technological narratives, policy issues, identity and institutional use, I note that three pieces of work in particular provided inspiration when considering the emerging data categories. These were Selwyn's (2000) argument that the Internet has potential as a surveillance tool, Oswell's (1998) discussion of children not only being at risk on-line but also a source of danger and Lawson and Comber's (2000a) assertion that the school Internet blurs conceptual boundaries. With regards to the risk literature I argue that a broad review of sociological perspectives on risk will provide some useful insights. Thus I consider Lupton's (1999) distinction between realist and social constructionist viewpoints, before introducing three differing perspectives, namely the risk discourse approach, "risk society" perspective and the cultural approach. I argue that with regards to school Internet use it was the cultural approach to risk, which includes the work of Douglas (1985, 1992, 1982 with Wildavsky) and Wynne (1989, 1996), that offered the most useful insights. In particular I focus upon two issues, the ability to distinguish between actual and perceived risks, and the role of expert / layperson knowledge. In drawing chapter two to a conclusion I make four claims that are relevant to this research. Namely that both staff and student risk narratives require consideration, that the question of who is in danger needs to be addressed, that a distinction needs to be drawn between actual and perceived risks and that school attempts to control Internet use need to be considered.

Having explained the research rationale and reviewed the relevant literature, I then consider in chapter three the research focus and methods. Thus, I outline the main research questions, touching upon issues such as staff / student perceptions of Internet risk, the reality of these dangers, and attempts to alleviate such risks and control the "net". Following on from this I describe the sampling techniques, describing how schools were chosen for this research and how individuals as well as locations were selected within these institutions. I also provide a brief sketch of all eight schools in which the research was carried out. After describing the sampling techniques, I briefly consider the case study approach to research before discussing the processes of observation, interviewing and content analysis. Having focused on the research methods, I then draw upon writings on grounded

theory and "subtle" realist ethnography in discussing how the data was analysed. Finally, I consider the two main ethical problems that emerged during the research. These were asking questions about potentially embarrassing subjects, such as on-line pornography and witnessing student abuse of the Internet.

Having set out the background to the research in the first three chapters the next three chapters are concerned with describing the staff / student risk perspectives. In chapter four I outline the concerns expressed by thirty staff who were interviewed across eight educational institutions. In addition to describing their concerns I seek to distinguish whether they saw the students and /or their institution as being at risk. I note that the majority of staff interviewed were concerned about on-line pornography and the dangers of chat-lines, while other issues such as hate engendering sites, websites encouraging experimentation, copyright and network security also created anxiety. Indeed of the thirty staff interviewed twenty-eight expressed concern about pornography, twenty-four about on-line chat rooms, three focused on "hate sites", two were worried about experimentation websites, seven considered the legal threat arising from copyright violation and nine discussed the dangers posed to network security. In discussing these concerns, staff drew variously upon the narratives of the "student-at-risk" and the "dangerous student". In conclusion, I argue that students engaging in hazardous Internet activities in the primary schools were seen solely as being at risk, while in the post-16 institution students were mainly perceived as a source of danger to the college. In secondary schools the narratives of the student being at risk and / or dangerous were used when describing on-line hazards.

The most notable feature of the student risk narrative detailed in chapter five is its almost non-existence on a verbal level. While sixty three students across eight institutions were asked about the problems and dangers that they perceived surrounding the Internet very few expressed concerns beyond issues of web searches producing too many hits, the pitch of websites and the reliability of on-line information. At four of the institutions, students did not express any concern about on-line dangers. I argue that this sparse narrative and the failure of students in four of the institutions to declare any perceived school Internet risks reflected

a genuine lack of anxiety about on-line hazards. The three issues that did emerge from the student interviews related to risks arising from pornographic material, on-line chat sites and doubts about the security of the school system. Thus eleven students discussed the issue of on-line pornography, five talked about problems relating to chat-lines and three expressed concern about network security. While I note that students aurally expressed few concerns about on-line risks I argue that some displayed non-verbal indications of anxiety about possible punishment arising from school Internet misuse. Thus students were observed engaging in a wide range of activities that could be viewed as attempts to avoid staff surveillance and subsequent punishment. For example students hid monitor screens, adjusted consoles so they could not easily be seen by observers, chose Internet machines in secluded corners, hid web pages behind other work, used other students' passwords and waited for unsupervised "windows of opportunity" to misuse the Internet.

Having described staff / student risk narratives I then seek in chapter six to illustrate how some of the categories used to describe risks arising from on-line activities were problematic. Thus, some staff and students disputed the labelling of certain material on the "web" as pornographic, racist, encouraging dangerous experimentation or infringing on copyright. Drawing on the concept of social construction I note that material and events might be interpreted differently depending upon a person's background. I also argue that interpretations of material may differ depending on the supervisor, user and the use to which such data is put (Resnick and Miller, 1996). Furthermore while interpretations and judgements are often made with reference to a host of surrounding signs the Internet potentially removes such references, blurring conceptual boundaries (Lawson and Comber, 2000a). Drawing upon these arguments I consider some practical examples where staff and students contested the labelling of on-line material as pornographic, hateful, encouraging experimentation or infringing copyright. In describing these issues I do not attempt to construct a framework for interpreting Internet misuse but rather seek to illustrate how social construction, issues of context and the nature of the Internet makes the labelling of certain on-line material problematic.

While chapters four, five and six focus upon describing staff / student risk perceptions, the next two chapters attempt to make a practical assessment of the actual dangers arising from school Internet use. In considering the issues of pornography, undesirable others, hate engendering sites and experimentation websites in chapter seven I draw upon the discourse of the "student-at-risk". Reviewing each of these risks individually, I consider the availability of on-line material, the incidents of students accessing such material in the schools studied and relevant events in wider society. I then draw this information together, consider possible consequences and make a judgement as to whether a risk is merely perceived or actual. In the case of the latter, I then seek to assess the likelihood of occurrence. Overall I conclude that children are not likely to suffer psychologically as a consequence of briefly viewing pornography on the school Internet and that whilst the dangers of on-line paedophiles, race hate sites and websites encouraging experimentation are actual, they offer a statistically remote risk.

Having considered the "student-at-risk" from on-line activities, I turn my attention in chapter eight to the "dangerous student", focusing upon the issues of school image, staff authority, copyright infringement and network security. Once again I describe occurrences in the schools studied before considering reported incidents in wider society. While I recognise the potential problems created by students misusing the Internet and sullying the school image, challenging staff authority or infringing copyright I find no evidence to suggest that these issues should be a source of great concern. Rather I note that the one Internet related threat plaguing both schools and wider society was the issue of network security being compromised. For the schools involved in the research I observe that this security problem was related to students "hacking" into the network or using one another's passwords.

Partly in an attempt to alleviate the actual and perceived risks arising from school Internet provision the eight educational institutions involved in the research made use of a range of control techniques. In particular the schools attempted to control student Internet use with rhetoric, exclusion of on-line material / students and surveillance. These attempts at control form the focus for chapters nine, ten and

eleven respectively. In chapter nine I focus upon the use of institutional rhetoric as an instrument of Internet control. I argue that the institutions attempted to construct rhetorically what constituted inappropriate Internet use through verbal communication, Acceptable Use Policies (AUPs), visual aids and third party pressure. I note that while in the primary schools verbal communication was used in a constructive manner to provide a framework for judging the appropriateness of websites, in the secondary and post-16 institutions it was primarily used to harangue students perceived as misusing the Internet. While Acceptable Use Policies were not adopted by the primary schools, I argue that the other schools in the research utilised them principally as protection against the Internet activities of "dangerous students". Despite the potential benefits of visual aids, I note that only one institution in the research used such devices in a direct attempt to construct rhetorically inappropriate Internet use. Finally with reference to third party pressure, in the form of relying upon parental influence and "netiquette", I highlight how such strategies were used in the schools studied to respond to students who had been caught misusing the Internet. In these cases, I argue that third party pressure was used as an instrument to control the activities of the "dangerous student". Indeed, in conclusion I note that while verbal communication was used constructively in primary schools to protect the "student-at-risk", in secondary and post-16 institutions such communication, AUPs, visual aids and third party pressure was used to safeguard the establishment from the "dangerous student".

In chapter ten I consider the use of filtering software and student exclusion as forms of Internet control. Thus, I note that with regard to the Internet, exclusion was used in two ways to alleviate risks. Dangerous material or individuals outside the school were kept out by filtering software, while students who intentionally misused the Internet were excluded from on-line activity, ICT rooms or even ultimately the school. While the first of these activities sought to ensure that risks which were external to the school remained outside of it, the second attempted to resituate an internal risk outside the area in which it posed a threat to the institution. In describing the exclusion of unsuitable on-line material I consider the use of "lists" that allow, deny or neutrally label websites, keyword matching, graphic content management programs and keyword monitoring

packages. Having described these applications, I then identify which ones were used by the primary, secondary and post-16 institutions. While I argue that the primary schools used filtering software to protect students perceived as being at risk, I note that in the secondary schools such products were also used to safeguard the institution against intentional Internet misuse. Indeed, I suggest that in the post-16 institution concern with the "dangerous student" was the prime motivation for using filtering software. In considering the exclusion of students, I argue that such action in the primary schools could be seen as an attempt to safeguard young students from unsuitable on-line material. In the post-primary institutions, while some policies such as the introduction of booking systems could be seen as attempts to allow all students to use the Internet, I argue that the dominant narrative was one of protecting the institution against the "dangerous student". Hence I observe that in the post-primary institutions policies such as locking rooms, disabling Internet access, throwing students off the Internet, evicting them from IT rooms and expelling them from school, all arose in response to incidents of intentional Internet misuse.

In chapter eleven I note that seeking to control Internet use the schools adopted strategies of physical and virtual surveillance. In considering the issue of surveillance, I initially focus on the writings of Foucault (1977) and Ball (2000), before considering the surveillance strategies adopted by the schools. With regards to physical surveillance I argue that three issues need to be considered, namely the identity of the observer, the focus of the observation and the use of space. I consider each of these issues in detail before examining how physical observation of Internet use was undertaken in the primary, secondary and post-16 institutions. I conclude that while surveillance in primary schools appeared to be concerned with the "student-at-risk", in post-primary schools the focus rested upon the activities of the "dangerous student". Two main forms of virtual surveillance of on-line activities existed in the fieldwork schools. Namely, software that recorded the addresses of websites and applications, such as Net Top Teacher, which allowed staff to view and control student Internet screens. While two schools in the research owned these latter devices, they were not used as surveillance tools. Having described the virtual surveillance methods adopted by schools in the research I note that on-line observation tended to rely on

computer logs of websites visited. Although computer logs existed in the primary schools, staff claimed that they were not used. In the secondary and post-16 institutions computer logs were used to reconstruct incidents of Internet misuse, identify the accessing of unsuitable websites and hold students accountable for their on-line actions. These observations led me to conclude that virtual surveillance in post-primary schools represented an attempt to control the activities of the "dangerous student".

In chapter twelve I draw together my research findings, outline the implications of these findings, reflect on the research process and indicate some possible areas for future research. With regards to school Internet use I argue that there are four elements of my research findings that might have important implications. Firstly, staff need to ask who is at risk when considering school Internet use. Considering both the "student-at-risk" and "dangerous student" narratives will enable them to clarify their concerns and take appropriate action. Secondly, while incidents of students accessing pornography or engaged in sexual on-line "chats" did occur in all the post-primary schools studied, no evidence suggested that psychological or reputation damage resulted. Thirdly, although a wide range of copyright infringements occurred in the schools involved in the research no prosecutions resulted. This situation suggests that companies are reluctant to prosecute schools for copyright infringement as long as the schools do not profit from such an act. Finally, attention should be focused on the issue of on-line security. If administration information such as staff reviews, reports or even salary information is stored on-line, staff need to be able to ensure the integrity of the local network from internal student "hackers".

Reflecting upon the research process and a critical engagement with sociological writings on risk, I argue that this thesis makes three main contributions to the sociology of risk literature. Firstly, it illustrates that if risk is to be comprehensively understood as part of both the natural and social worlds, analysis needs to include not only risk narratives and an assessment of the actual dangers but also a description of attempts to control risks. Secondly, within this broad approach, this research shows that risk narratives need to be considered from a hermeneutic perspective. Finally, in assessing risks I argue that there is a

need to move the focus away from risk processes to include consideration of risk outcomes.

Part One

Research Background

In chapter one I detail the rationale for undertaking research into the risks arising from school Internet use. In chapter two I review literature on the social impacts of the Internet and the sociology of risk before drawing together some common themes. Finally in chapter three I describe the research focus, sampling procedure and methods used.

Chapter One

The rationale for research into risks arising from school Internet use

Introduction

The scale and speed at which forms of information communication technology known variously as the Internet, the World Wide Web and electronic mail have entered ordinary life in the economically developed countries is striking. Despite its popularity and the rate at which its use has spread, little research has been undertaken assessing the social impact of such technology. The small amount of education-based research that has focused upon the Internet has tended to concentrate on issues of integration and effective use. Inevitably with new technology the first concern is often learning to use it effectively. Yet in spite of widespread media concern about the possible risks lurking on-line there has been a general lack of sociological research considering the dangers which such technology introduces into schools. The need for information about risks arising from school Internet use becomes more urgent when set in the context of current educational policy such as the National Grid for Learning (NGfL) which seeks to introduce the "net" to all 30,000 schools in Britain by 2002. One might be forgiven for believing that research focusing upon the dangers and the "darker side" of the Internet is inevitably negative, dystopian and unhelpful to educators. Yet, informing teachers about on-line hazards, exposing unfounded fears and providing some balance to a narrative that constructs the Internet as a pedagogic saviour is a worthwhile project in itself.

In considering the need for research into the risks arising from school Internet use five questions need to be addressed:

- Why study the social impact of the Internet?
- Why situate the study of Internet use in schools?
- Why use the concept of risk?
- Why associate risk with schools?

- Why focus upon risks arising from school Internet use?

In answering the first question I argue that the Internet is claimed to be novel, rapidly growing, transformative technology. While the first of these claims is easily substantiated with a brief consideration of the history of the Internet and the second one can be accepted following a brief analysis of the number of Internet users as well as websites, the third claim is more problematic. Regardless of the validity of descriptions of the Internet as transformative technology, I maintain that this narrative itself is significant insofar as it can be situated within a wider technological discourse that informs government policy formation in the United Kingdom (UK). Indeed government policy is a key consideration in answering the second question, regarding the situating of the study of Internet use in schools. In Britain the Labour government has pursued a policy of establishing a "National Grid for Learning" (NGfL) seeking to connect all schools in Britain to the Internet by 2002, at a cost in excess of £700 million. The impact that the Internet might have in over 30,000 schools in Britain deserves attention. In answering the third question, why use the concept of risk, I maintain that not only is risk a feature of society, one which academics have increasingly focused upon, but that it also provides a useful conceptual framework for considering fears and dangers. In addressing the fourth question relating to the links between schools and risks I argue that following incidents such as the Dunblane shootings, the murder of the headmaster Philip Lawrence and massacres in educational institutions in the United States, schools have become perceived as "risky" environments. Finally in justifying why I specifically concentrated upon risks arising from school Internet use I explain that this focus emerged from the research, which in turn drew my attention to the wider Internet risk narratives evident in the mass media, government documentation and special interest group publications. Furthermore I note that there is a lack of research into the possible dangers arising from school Internet use.

It should be noted that this chapter offers a rational reconstruction of a messier research process. The focus on Internet risks emerged from my initial fieldwork in schools and some background reading of relevant documents. Additionally I had some existing knowledge of the risk literature, which sensitised me to key

issues and enabled me to see the relevance of this sociological work to the emerging issues. Thus this chapter should not be seen as a linear historical description of the research process but rather as a logical reconstruction, which seeks to highlight issues which were instrumental in formulating the research focus.

1. Why study the social impact of the Internet?

In considering the social impact of the Internet three distinct claims need to be examined. These are that the Internet is novel, that its use has grown substantially in recent years and that it can be considered as transformative technology. In assessing these assertions, I will briefly describe the Internets history and the increase in the number of Internet users and websites in recent years. Finally, I will argue that, despite little empirical evidence to support claims about the transformative nature of the Internet, this discourse still informs UK government policy decisions.

Despite many debates about the Internet there often exists a conceptual vagueness as to its constituent parts. To avoid such ambiguities I will define the key terms associated with the Internet before briefly relating their respective histories. Simply put the Internet (or "net" as it is sometimes called) is a world-wide network of computer networks, connected by telephone communication systems (BECTa, 1998: 61). While, due to its vast commercial success, the World Wide Web (often abbreviated to WWW or the "web") has become synonymous with the Internet, it differs in that it is protocol software that rides on the back of the existing Internet structure. Like the web electronic mail (e-mail) and "net" newsgroups are further examples of software applications that use the infrastructure of the Internet to function. While the Internet and the web will be treated as distinctive entities in the following brief historical analysis in subsequent sections and chapters of this thesis the terms will be used synonymously, unless otherwise stated. The justification for this lies in their common interchangeable use, in schools, the mass media, government policy and academic literature.

1.1 A brief history of the Internet

The Internet has its origins in the cold war space race of the 1950s. The United States (US) Advanced Research Projects Agency (ARPA) is commonly credited as the creative force behind the Internet. ARPA was formed in response to fears of Soviet technological superiority following the launch into orbit of the Soviet Union satellite Sputnik on 4th October 1957. Having ceded its aerospace remit and most of its funding to the newly formed National Aeronautics and Space Administration (NASA) in late 1958 ARPA focused on "blue sky" research, with subsequent heads of its Information Technology Division encouraging research into computer mediated communication. Despite a partially successful attempt to link two machines at opposite ends of the US in 1965 it was not until four years later that ARPA employees succeeded in constructing a reliable computer network capable of exchanging computer files and messages using existing telephone lines. While ARPANET remained a military venture, systems that allowed the public access to computer mediated communication followed. For example in 1978 the French Telephone Company created the MINITEL system, allowing individuals to videotext messages to one another. In the US in 1979 Bell Labs released a communications program which allowed one computer to call another via a telephone and deliver software to it down the line.

While computer mediated communication steadily grew it was the creation of the World Wide Web which was largely responsible for the phenomenal growth of "net" use in the 1990's. While on a consultancy at CERN, the European Organization for Nuclear Research, Tim Berners-Lee realised that keeping track of diverse information was an institutional problem. His solution to this problem was to design a program called a browser that provided a virtual window through which the user could see a web of linked sources on the Internet. Working with Nicola Pellow, a technical student, he drew up demonstration versions of both browsers and web severs, allowing users to access various files and newsgroups. By March 1991 the WWW software was available to a limited audience at CERN and in December of the same year the arrival of the World Wide Web was announced to the world. Despite steady growth in the use of the World Wide Web it was not until the launch of Mosaic in the spring of 1993 that the web

started to grow rapidly. Created by Marc Andreesen and other students and staff at the University of Illinois' National Centre for Supercomputing Applications (NCSA), Mosaic was a point and click browser with a graphical user interface. The software was available free and significantly allowed web pages to include images side by side with the text for the first time.

From its early origins as a storage and messaging device the Internet's uses have grown significantly. In addition to the retrieval of images, information and sound files the Internet allows real time communication through typing, voice software and web cameras. Not only can individuals retrieve data and communicate using the Internet, but with the increasing availability of simple to use website construction packages they can also publish information. Indeed, it is argued that in schools the Internet enables students to access educational resources held on the web, communicate electronically via e-mail, on-line chat or video-conferencing, and create information for others to access (BECTa, 1998: 18).

As the Internet is a relatively new invention there has been little time for reflection on its social impact. Yet its recent history and novel uses suggest that the Internet would be a rewarding focus for social research. Such claims are reinforced when one considers the growth in the number of people using the Internet and the increasing array of websites that they have access too.

1.2 The growth in Internet use

The Internet has grown substantially both in terms of the number of users and the resources available on the web. Indeed the Internet's pace of adoption eclipses all technologies before it. While radio existed for 38 years before it gained 50 million listeners and television took 13 years to reach this point, the Internet crossed this line in four years. While three million people were connected to the Internet in 1994 by March 1998 the figure had increased to 119 million (Moschovitis et al, 1999). Traffic on the Internet doubles every hundred days (Joo, 1999: 245) Furthermore the number of websites grew dramatically from 130 in June 1993 to 10,022 in December 1994 (Moschovitis et al, 1999). This growth has largely been a reflection of the reduction of the cost of the equipment

necessary to go on-line, the user friendliness of menu driven operating systems and the burgeoning economic, educational and recreational uses of the "net".

Ultimately this substantial growth in Internet use might suggest that its impact in economically developed countries will be widely felt. Such considerations suggest that there is a growing need to undertake sociological research into the impact of the Internet. Claims that such technology has led to a radical transformation in contemporary society deserve attention. Hence I will now consider claims that the Internet is part of a technological vanguard that has led to a radical change in contemporary Western society.

1.3 The Internet as transformative technology

Writings about the social impact of the Internet often embrace the meta-narrative asserting that Western society has gone through a radical transformation in recent years, changing from an industrial to a "post-industrial" or "information society". Arguments about "information society" have their roots in the writings of Bell (1976), Toffler (1970, 1980, 1990) and Negroponte (1995). These authors maintain that production is no longer centred on goods but rather on the flows of information, enabled largely by the development of complex information communication technology. While arguments about "information society" do not focus exclusively on the Internet, such technology is at the heart of claims that society has radically changed.

The arguments that an "information society" has emerged have been criticised as anecdotal and lacking in empirical evidence. Indeed Webster (1995) argues that claims that the UK has transformed into an information society are untenable when assessed using technological, economic, occupational, spatial or cultural criteria. Nevertheless despite a comprehensive and systematic critique (e.g. Kumar, 1995; Webster, 1995) works claiming that the West can now be seen as an "information society" remain influential (Webster, 1999: 80). Thus academic publications about the Internet proclaim a technological "revolution" (e.g. Baym, 1998; Rheinegold, 1994; McLaughlin, Osborne and Ellison, 1997), while political discourse focuses on the need to create "tomorrow's information

society" (Conservative Party, 1997; Labour Party, 1997), and advertisers herald the transformative power of the "Net".

1.4 Summary

I have argued that research should be undertaken into the Internet as it is a recent, novel invention. Furthermore, little is known about its social impact. The growth of Internet use in recent years, both in terms of the number of users and on-line resources, has been substantial. Thus the Internet itself provides a potentially rich seam for social research. Finally regardless of the validity of claims that the Internet is transformative technology the narrative itself is sufficiently influential to warrant research in this area. Indeed this last point is relevant when considering the reasons for undertaking research about the Internet in schools.

2. Why situate research focusing on Internet use in schools?

This research on Internet use was situated within schools in response to government policy, in particular the National Grid for Learning, and widespread Internet provision arising from educational institutions funding their own connectivity.

2.1 The National Grid for Learning

The UK government has been an active agent in encouraging Internet use in business, education and wider society. Recent government policy initiatives have attempted to introduce Internet access into schools, on the basis that it will provide a wealth of learning resources and develop essential technological skills. Thus the National Grid for Learning (NGfL), introduced in the consultation document *Connecting the Learning Society* (DfEE, 1997a), represents a £700 million investment program aimed at connecting all of Britain's 30,000 schools to the Internet by 2002. Additionally a further £230 million of Lottery money has been allocated to the National Opportunities Fund with the aim of training all teachers to use this new technology. Other government policies for the, so-called, "Learning Grid" include the creation of various on-line resources for

schools, the most notable of which is the "Virtual Teacher Centre". This website provides access to educational software and curriculum material, as well as providing a forum for teacher discussion and dissemination of good educational practice. Since the Grid's launch in October 1997 additional elements have been regularly announced, including a £50 million program to digitise and provide on-line access to every major historical artefact in the country's museums and libraries, the provision of laptop computers to nearly 10,000 teachers and tax concessions for teachers purchasing computers.

The NGfL initiative has not only been central in introducing the Internet into schools and encouraging its acceptance in the wider teaching community but has also been influential in constructing a narrative regarding the need for school Internet access, "moving the education service into the twenty first century and creating a connected society" (Blunkett, 1997: 11). By positioning the NGfL within the narrative of the "information society" the Labour government clearly seeks to signify the wider societal significance of this policy (Selwyn, 1999a: 66). Additionally NGfL documentation has also attempted to construct the "Learning Grid" as central to citizenship, employment opportunities and education.

In education the Internet is not only promoted as a pedagogic saviour, improving educational provision, but also as "the teachers friend", potentially reducing the administrative workload (Selwyn, 1999a: 68-9).

If government targets are met over 30,000 schools will have Internet access by 2002. The introduction of the Internet into so many schools is a source of research interest. Yet as I shall now argue even without government initiatives, such as the NGfL, Internet provision would still exist in schools.

2.2 Alternative sources of funding for school Internet provision

Recognising the educational potential of the Internet some schools have drawn upon their own resources and sponsorship from industry to provide on-line access. The nature of the NGfL funding cycle has meant that some schools faced

the possibility of waiting four years before they were allocated money. In a competitive educational market it is hardly surprising that some schools sought to fund their own Internet access rather than waiting for their turn in the funding cycle. The apparent eagerness of schools to be on-line regardless of government funding suggests that some institutions would have proved suitable sites for research on Internet use regardless of initiatives such as the NGfL.

2.3 Summary

I have argued that schools provide potentially fruitful field sites for research into Internet use. This is a consequence of government policies and schools own efforts to provide Internet access. Having established why this research is focused upon the Internet in schools I will now consider why the concept of risk was adopted as a sociological framework.

3. Why use the concept of risk?

Before asserting that risk is an important concept insofar as it is a feature of contemporary society, a focus for recent academic writings and provides a useful sociological framework for research it is important to define the term. According to Furedi:

> Risk refers to the probability of damage, injury, illness, death or other misfortune associated with a hazard. Hazards are generally defined to mean a threat to people and what they value (Furedi, 1997: 17).

In this sense risk is associated with danger and threats to the individual and their property. The concept of risk is considered in detail in chapter two.

3.1 Risk as a feature of contemporary society

As Caplan (2000: 1) notes at the start of the new millennium risk is a topic that is difficult to ignore. Concern about food production has proliferated, with arguments raging about diverse subjects such as genetically modified crops, listeria, Creutzfeldt-Jakob Disease (CJD) and Foot and Mouth Disease. Protests

about global pollution grow as individuals come to realise that the negative effects of industrialisation might be felt for generations to come. Following recent disasters even mundane experiences such as rail travel have been perceptually transformed into hazardous undertakings. One might be forgiven for thinking that the contemporary world is much more dangerous than the one that existed a few decades ago. However, as Giddens (1991) notes despite the increase of global level risks, it is not necessarily that society is more dangerous, rather people have become "risk obsessed". From security systems to vitamin supplements, risk has become a multi-billion dollar business (Bauman, 1993).

3.2 The growth of sociological writings on risk

Within academia attention has recently focused upon the sociology of risk. While the anthropologist Mary Douglas has written extensively on the subject of risk, it is the more recent work of Beck (1992) and Giddens (1991) on "risk society" that appears to have ignited current academic interest in the concept. Arguably, this interest has been stimulated by the theoretical framework of the "risk society" thesis that combines an interest in issues such as social transformation and globalisation with concern for the environment and health. Arguably the appeal of the "risk society" thesis lies in its combination of a meta-theoretical perspective with a green consciousness. Furthermore, attempts to explain changes in contemporary society on a global level can be seen as having an appeal to those sociologists trying to provide holistic explanations for contemporary problems. These issues are dealt with in more detail in chapter two.

3.3 Risk as a useful sociological framework

Theoretically the sociology of risk lends itself to a consideration of the narratives surrounding the perception of danger and the assessment of hazards. It allows for the examination of widely differing discourses about perceived dangers. Through adopting sociologically informed perspectives it is possible to interpret and assess these risk narratives from a variety of viewpoints. Additionally there exists the possibility of attempting to empirically measure risks, over a given time

period, and subsequently differentiate between dangers that are merely perceived and those that are actual. Central to risk is the idea that something can be done to alleviate the danger, normally through observation and control. Thus the concept of risk allows for a consideration of control and surveillance issues.

3.4 Summary

I have argued that risk is a potentially rewarding focus for research in that it is a notable feature of contemporary society, upon which sociologists have recently focused, that provides a useful theoretical framework for research. While little of the contemporary sociological writings on risk focus on education I would nevertheless argue that in recent years schools have become perceived as "risk environments".

4 Why associate risk with schools?

There is a tendency for sociological research into risk to focus upon issues such as ecological dangers (e.g. Wynne, 1996) or health hazards (e.g. Day, 2000; Bujra, 2000). Within this context, it could be asked why research into risk in schools might be fruitful. In addressing this question I will argue that following recent high-profile occurrences, in the UK and US, schools have become perceived as "risky" places. Furthermore I will note that reactions to such perceptions in the form of safety and surveillance measures can be seen as constructing schools as environments where the reduction of risk is a central concern.

4.1 Schools as "risk environments"

Incidents such as the killing of sixteen students and their teacher at Dunblane Primary School, the murder of headmaster Philip Lawrence by a schoolboy wielding a knife, the knife attack on a primary school class in Wolverhampton, the fatal stabbing of student Damilola Taylor while walking home from school and the collapse of the Ridings school in West Yorkshire have all gone some way to constructing a perception of schools as being "risky" places (Thompson,

1998). Despite a difference in gun laws, incidents in the US have arguably fed into this general perception of schools as risk environments. The reporting in the international media of incidents such as the killing of thirteen people at Columbine High School in Littleton, Colorado in April 1999, the fatal shooting of four girls and a teacher at a middle school in Jonesboro, Arkansas in March 1999, and the murder of two teenagers at Thuston High school in Springfield, Oregon in May 1998, help to paint a bleak picture of schools. Indeed the list of recent killings and non-fatal shootings in US schools is a long one.

While it might be argued that British schools differ markedly from their US counterparts two points need to be made. Firstly, media images of violence and danger situated in schools help to create an association between schools and risk. Secondly, students have largely perpetrated the incidents of violence in post-primary educational institutions in both Britain and the US. I argue that in this context students might not only be "at risk" from violence or abuse in schools, but also might be seen as a source of that risk, insofar as they are "dangerous". This last point provides one key focus for this research and will be considered in more detail later in the thesis.

Arguably it is not just violence but also other issues such as child abuse, abduction, road safety outside schools, and the spread of illnesses, such as meningitis and tuberculosis, which help to construct UK schools as risk environments. Indeed, it can be argued that we live in a society that has become more risk conscious in recent years, where parents are reluctant to let children walk home alone from school, or fearful of other adults dealing with their children.

In response to these dangers schools have adopted a variety of security measures. Thus, close circuit television cameras (CCTV), security doors, intercoms, identification badges and the signing in of visitors are in evidence in many educational facilities. Risk avoidance in schools has become big business. As Frank Furedi in his book *Culture of Fear* remarks:

> In the UK safety in schools is a big issue. The comprehensive range of cameras, swipe cards, and other security measures that are now routine make many schools look like minimum security prisons ... risk avoidance has become an important theme in political debate and social action (Furedi, 1997: 3).

While adopting security measures in schools may reduce threats to student safety they also potentially change the atmosphere of such establishments. By introducing greater security measures schools are implicitly accepting that they have become places of "risk". Yet it should be reiterated that schools are not constructed as "risk environments" solely in response to incursions from the outside world. Rather students and staff are also a potential source of danger. Thus in some situations the student becomes the focus of surveillance and control. For example libraries or ICT suites may have CCTV to discourage students from vandalism or theft.

4.2 Summary

Events in both the UK and US can be seen as feeding public perceptions of schools as dangerous places. Furthermore, the association of murder, child abuse, abduction and the spread of infectious diseases with schools helps to reconstruct them as "risk environments". In addressing the final major question, why concentrate upon risks arising from Internet use in schools, I will highlight why the language of risk is appropriate in describing Internet use.

5. Why focus upon risks arising from school Internet use?

Having produced a rationale for sociological research into Internet use in the wider society, as well as within schools, it now remains for me to provide a justification for focusing upon risks arising from Internet use. While the primary stimulus to study Internet risk arose from the research itself, government, mass media and special interest group narratives subsequently reinforced this focus. Additionally the lack of research into the area of school Internet risks was a motivating factor. In explaining why I focused on Internet risks each of these

issues, research data, government discourse, mass media reports, special interest group publications and the lack of existing research will now be considered.

5.1 Emergent focus from research

Initially I intended to focus my research on issues of power and the use of Information Communication Technology (ICT) within schools. However, within the first few months of fieldwork my focus shifted, and became more defined, as I gathered data which indicated that there was concern about the possible risks arising from school Internet use. Thus teachers expressed fear that children might be harmed by on-line pornography, seduced by strangers in cyber-chat rooms, influenced by racist websites or tempted to construct explosives following on-line recipes. Additionally some staff expressed concern about the damage that the institution might suffer if the students violated copyright, e-mailed offensive messages to outsiders, were exposed in the media as accessing pornography in school or managed to use the Internet to gain access to restricted information. Reported incidents of students accessing pornography, "hacking" into the school computer network and arranging to meet up with strangers encountered on-line suggested that some of these risks might be real. While students were less vocal in addressing the issue of on-line dangers, observation of their behaviour over time suggested that they saw punishment for Internet misuse as something of a hazard. All these issues are dealt with in detail later in the thesis.

Thus the primary focus upon Internet risks can be seen as having emerged from the fieldwork. Yet this interest was also stimulated through the reading of general documents and media reports relating to Internet use. While I was aware of some of the sociological literature on risk prior to the start of the research, it was only as data was gathered from my initial fieldwork sites that I started to consider the conceptual relevance of risk. Having some pre-existing familiarity with the risk literature I was able to see the potential usefulness and significance of this conceptual framework. Indeed as the research focus became more defined I started to become aware of the risk narratives evident in government documentation, media reports and the publications of special interest groups. These narratives will now be considered.

5.2 Internet risk narratives within wider society

While the potential benefits of the Internet are widely heralded by the government, advertisers for Internet services and the media there is also a muted recognition of on-line dangers. The following focus on the Internet risk narratives of government bodies, the mass media and voluntary organisation should not be taken as an indication of the relative importance of these issues of effective use and on-line risks but rather as a consideration of an area that is largely neglected in academic research. Thus I will now consider the concern with on-line dangers evident in government documentation, media coverage and the publications of special interest groups.

5.2.a Government narratives on Internet risks

In analysing government risk discourses it is necessary to distinguish between the European Commission, the UK national government and local government. This will provide an insight into some of the key organisations involved in constructing the "net" through discourse.

Policy documentation at the European level addressing the possible dangers of the Internet have tended to be couched in terms of illegal and harmful content (European Commission, 1996a; European Commission, 1996b). Illegal material in this context is defined as:

> A general category of material that violates human dignity, primarily consisting of child pornography, extreme gratuitous violence and incitement to racial or other hatred, discrimination, and violence (European Commission, 1996a: 6).

Harmful material, while not forbidden by national law, is restricted to adults only as it might affect the physical and mental development of minors and might offend certain other users (European Commission, 1996b). Policies addressing this concern with harmful and illegal Internet content have tended to construct the problem largely in terms of pornographic material of a deviant nature, such as sado-masochism, bondage, paedophilia and zoophilia, and the activities of

paedophiles (Commission, 1996a: Commission, 1996b: European Parliament, 1999). While it is the responsibility of member states to ensure the application of existing laws, because of the highly decentralised and transnational nature of the Internet concrete measures to ensure co-operation between member states have been launched. Thus there have been numerous international initiatives promoting safer use of the Internet, through creating a European network of "policing" hotlines, encouraging self regulation and developing filtering / rating systems (European Parliament, 1999). Yet concern at the European level with on-line risks should be put in context. It has been recognised not only that the majority of Internet usage is totally legitimate (European Commission, 1996b) but also that the "net" has the potential for:

> [E]mpowering citizens and educators, lowering the barriers to creation and distribution of content, [and] offering universal access to even richer sources of digital information (European Commission, 1996a).

The British government has been criticised for concentrating on the potential benefits of the Internet at the expense of informed discussion of the on-line risks to children (Moran-Ellis and Cooper, 2000: para 2.4). While there has been limited government recognition of on-line dangers it has tended to be versed in quite abstract terms. For example the Department of Education and Employment issued a document aimed at parents and schools entitled *Superhighway Safety: Safe Use of the Internet* (DfEE, 1999). This package, which included a Disney endorsed poster offering five tips for safe "surfing", focused upon issues such as, Internet filtering systems, Acceptable Use Policies and general safety on the "net". Yet references to specific concerns such as pornography, race hate websites and the on-line activities of paedophiles were conspicuous by their absence. Other publications sponsored by government bodies such as the British Educational Communications and Technology agency (BECTa), whose role is to ensure that students leave school with the ICT skills for the twenty-first century, has equally tended to largely ignore risks arising from Internet use. Thus *Connecting Schools, Networking People* (BECTa, 1998) a sixty six page report on ICT planning, purchasing and good practice dedicates only a single page to the issue of undesirable material. While the report is illustrated with thirty-one case studies none of these elaborate on the issue of Internet risks.

At a local level education authorities have issued guidelines for appropriate Internet use, as well as exemplars of Acceptable Use Policies for schools to adapt and adopt. For example, Shropshire Local Education Authority (LEA) has sent a ten page code of practice to all its schools, while Derbyshire LEA has formulated a similar policy (Times Educational Supplement, 03.03.00). Interestingly these documents are concerned not only with student Internet use but also with possible misuse by staff.

Overall it can be seen that some concern exists at a government level regarding the dangers arising from Internet misuse. Such narratives of on-line dangers provide a rationale for this research.

5.2.b Mass media coverage of Internet risks

Media coverage of the risks arising from Internet use has been labelled as exaggerated, sensationalistic, and inciting moral panic (Akdeniz, 1997; Lawson & Comber, 2000b). A brief examination of how the "net" is presented through films will provide an insight into the media's role in constructing the Internet as a risk environment. I will then briefly consider some news headlines to illustrate media concerns about the Internet.

Hollywood has tended to concentrate on the negative side of the Internet in film depictions. For example, in *Wargames*, a film made when the Internet was still in its infancy, the main character almost triggers a nuclear conflict through his on-line "hacking" activities. More recent depictions of the Internet in films such as *The Net*, starring Sandra Bullock correlate the Internet with sexual harassment and rape (Furedi, 1997: 77). Even the romantic comedy *You've Got Mail,* starring Tom Hanks and Meg Ryan, which portrays an on-line romance hints at disturbing, sinister possibilities.

The news media have done little to challenge these Hollywood presentations of the "net". Rather the Internet tends to be presented as the haunt of paedophiles or a pornographic library to which children have easy access. Headlines in the British media such as "Teenage students rapped over school porn network"

(Sunday People, 18.10.98), "Porn risk to children". (Telegraph, 29.06.00), "Teachers' fear over Internet porn" (BBC News On-Line, 09.04.98) and "Net porn warning for pupils" (BBC News On-Line, 10.10.99) convey a sense of the Internet as dangerous. Furthermore these stories situate the problem of accessing unsuitable on-line material firmly within schools. Yet while the mass media portray the Internet as potentially dangerous they also seek to promote their own commercial and educational websites. This reflects competing tensions within which the Internet is seen primarily either as an educational tool aiding childrens' learning or a threatening, dangerous environment. Remarking upon these views Brooke notes that in the media:

> Mention children and the Internet in the same sentence and you either get the rosy picture of learning and childhood exploration, or anxiety about the corruption of innocent minds (Telegraph, 29.06.00).

In a media environment where sensation attracts consumers it is perhaps unsurprising if the "dark side" of the web receives prominent attention.

Carol Vodermann, a presenter and celebrity, argued on the *Tonight with Trevor McDonald* (25.10.00) television programme that the Internet had become a "candystore for paedophiles" with children being "targeted and groomed for abuse" (Telegraph, 25.10.00). Other reports such as "Cyber chat brings teen fantasies to life" (Times Educational Supplement, 17.03.00), "Children at risk from 'net' friends" (Telegraph, 07.08.00) and "Paedophiles calling a fifth of children on net" (Sunday Telegraph, 03.12.00) help to construct a narrative in which the Internet is seemingly populated by child sex abusers.

Overall the media tend to present the Internet as a risk environment, portraying it as a hunting ground for paedophiles and, through the easy availability of pornography on-line, a corrupting influence on children. Indeed concern about the dangers threatening children is at the heart of much discussion about the Internet. Focusing upon this concern I will consider the fears expressed by NCH Action for Children, a highly vocal special interest group that has played a role in the discursive construction of the Internet.

5.2.c Special interest groups and the Internet

External to the government and the Internet industry are a whole range of bodies set up to promote particular issues, such as child safety, freedom of speech, safeguarding moral standards or promoting minority interests. While I have no intention of providing an exhaustive list of such special interest groups, one group in particular, the NCH Action for Children deserves brief consideration insofar as it has played a significant part in labelling the Internet as risky.

NCH Action for Children, one of the UK's largest children's charities, deals with issues of child welfare and protection. While recognising the transformative potential of the Internet, and expressing concern for children who do not have access to the technology, the main focus of their booklet *Children on the Internet: Opportunities and Hazards* (1998) is on-line dangers. Indeed in an emotive, if somewhat sensationalistic overview, the Chief Executive, Deryck Mead, asserts that:

> Hardly a week now seems to go by without yet another Internet case involving children in some way or other coming to light. No-one wants the Internet to become synonymous with pornography or dangers, but that's the way things could easily go unless we can reverse the tide ... there are denizens of the dark out there ... (Mead, 1998:8).

Mead's (1998) concern focuses sharply upon the on-line activities of paedophiles and the possibilities of children accessing harmful pornographic material. Indeed *Children on the Internet: Opportunities and Hazards* (1998) firmly situates children as being at risk from physical and psychological abuse arising from on-line activities.

5.3 Lack of existing research into school Internet risks

The research focus on risk and Internet use emerged primarily from initial fieldwork, and was reinforced by the existence of a distinctive public narrative emphasising harmful and illegal on-line activity. A pre-existing familiarity with the writings of Douglas, Beck and Giddens sensitised me to the concept of risk

while enabling me to see the relevance of these writings to the "emerging issues". A further reason for focusing the research upon risk lay in the relative absence of existing studies in this area. Indeed beyond Oswell's (1998) consideration of the place of childhood in Internet content regulation and Lawson and Chamber's (2000a) analysis of the censorship of the Internet in schools there is a lack of sociological research into the issue of unsuitable Internet use. This issue will be addressed in more detail when I review the sociological literature focusing upon Internet use in the next chapter.

5.4 Summary

The concern with risks arising from school Internet use emerged from the early phases of my research both through the fieldwork and initial broad background reading. Through examining government, media and special interest group risk narratives it can be seen that a concern exists about the potential dangers arising from children using the Internet. This subject of potential on-line dangers is one that has been largely ignored in academic research.

Conclusion

In providing a rationale for research into the risks arising from school Internet use I have provided justifications for focusing upon the Internet, situating the research in school, using risk as a conceptual framework, linking the concept of risk with schools and finally studying dangers arising from "net" use in school. Thus I have considered claims that the Internet is novel, has grown in use, and is transformative. While I argued that the last of these claims was difficult to establish I maintained that this narrative of the Internet as transformative technology was nevertheless used in UK government policy discourse. Part of this government policy, the National Grid for Learning provided a major impetus for research into school Internet use insofar as it aims to provide in excess of 30,000 schools with Internet provision by 2002. Nevertheless, I also maintained that schools are often keen to gain on-line access regardless of government funding. Focusing upon risk I argued that it is a valuable concept insofar as it can be seen as a feature of contemporary life, a developing concern for sociologists

and a useful framework for assessing danger. Furthermore I maintained that following highly publicised incidents of violence, concerns about the welfare of students and the increased introduction of security measures, schools have become constructed as "risk environments". Having noted that my concern with school Internet risks emerged from my initial research, I considered the concerns evident in government discourse, media coverage and the publications of some special interest groups. The final reason I gave for undertaking research into the risks arising from school Internet use was that the issue has been largely ignored. Indeed this lack of academic writing focusing on the risks arising from school Internet use is a major concern in the following chapter.

Having considered the rationale for research into risks arising from school Internet use I will focus upon the sociological literature about both the Internet and risk in chapter two.

Chapter Two

The Sociology of the Internet and risk

Introduction

In the previous chapter I presented a rationale for carrying out research into the risks arising from school Internet use. Thus, I maintained that communication information technology was novel, rapidly growing and heralded as transformative. Furthermore, I argued that as a result of the NGfL initiative all schools in Britain should have on-line provision by 2002. While noting that schools had become labelled as risk environments, I argued that contemporary society was risk-focused, as reflected in some recent sociological writings. Finally, I remarked that the research focus grew out of initial fieldwork in schools and was further developed through reading government documentation, mass media reports and interest group publications on Internet use.

While there is a growing body of work on the social impact of the Internet and a substantial range of writing on the sociology of risk, there is an absence of research that incorporates both of these issues. Lacking literature that combines a concern with both Internet use and risk I argue that it is worthwhile considering these two areas separately before seeking to make connections and draw out common themes.

Within the sociological literature four broad themes that have relevance to the school Internet can be identified. Namely, technological meta-narratives, policy issues, the social construction of identity and institutional Internet use. I will consider writings within each of these groupings in turn, highlighting how certain arguments informed my research. In concluding this literature review on Internet sociology I draw attention to three particular pieces of work, Selwyn's (2000) observation that the Internet fulfils a role as an effective surveillance tool, Oswell's (1998) consideration that children on-line are not merely at risk but also potentially dangerous and Lawson and Comber's (2000a) assertion that the school Internet blurs boundaries.

While there is no literature that specifically focuses upon the risks arising from Internet use, I argue that a broad review of sociological perspectives on risk will provide some useful insights. In the review of sociological writings on risk, I first draw on Lupton's distinction between realist and social constructionist perspectives, before introducing three broad analytical schools. These are the risk discourse approach, influenced by the writings of Foucault, the "risk society" perspective, represented in the arguments of Beck and Giddens, and the cultural approach, found in the work of Douglas and Wynne. I argue that with regards to school Internet use it is the third of these perspectives, the cultural approach to risk, which offered the most useful conceptual insights. In concluding my review of the key sociological perspectives on risk I draw attention to two features of the cultural approach, the ability to distinguish between actual and perceived risks, and the role of expert / layperson knowledge.

In drawing this chapter to a conclusion I combine the various insights gained from the Internet and risk literature and make four assertions that are relevant to this research. Namely that there is a need to describe both staff and student risk narratives, that the question must be addressed of whom is actually in danger, that a distinction needs to be drawn between actual and perceived risks and that school attempts to alleviate the dangers arising from Internet use need to be considered.

Importantly it should be noted that although my pre-existing knowledge of elements of the risk literature sensitised me to some of the key issues, the categories and findings that I discuss later in this thesis emerged from the data. Thus, the literature considered in this chapter offered inspiration when I was sorting through and analysing the research data.

1. The sociology of the Internet

Four broad themes can be identified within the sociological literature about the Internet, relating to technological narratives, policy, on-line identity and institutional use. I do not intend that these concerns be seen in isolation but rather as part of an emerging tapestry of academic work. In order to make sense of these

themes each will be addressed in turn, referring to general illustrative writings, before focusing more specifically on those pieces of work that situate the Internet within education. Thus in considering technological narratives I will touch upon arguments about the emergence of an "information society", drawing upon the work of Bell, Toffler and Webster. With regard to Internet related policy issues I will focus on the writings of Selwyn on the surveillance potential of the NGfL, Moran-Ellis and Cooper's criticisms of the simplistic construction of childhood in NGfL literature, and Oswell's distinction between the various narratives of the on-line child as victim, at risk or dangerous. In examining arguments about the social construction of on-line identity I will draw upon Joo's (1999) discussion of culture on the web as well as Hesketh and Selwyn's (1999) article on the electronic reconstruction of school identities. Finally, in reviewing institutional Internet use I will concentrate upon the work of Lawson and Comber on school Internet censorship and the blurring of boundaries.

1.1 Technological narratives

Narratives that consider the social impact of technology, such as the Internet, tend to draw, either implicitly or explicitly, upon writings about the emergence of an "information society". After briefly considering examples of work by Bell and Toffler, I will review Webster and Castell's criticisms of these "information society" arguments.

Since the 1970s there has been a growing body of sociological work either proclaiming or contesting that the nature of Western society has radically changed due to the increasing prevalence of information technology and the subsequent growth of information flows. Arguments about the emergence of "information society" have their roots in Bell's (1976) theory of a post-industrial society, in which he asserts that industrial society had been eclipsed by an information society, where the primary focus of production is informational. Although Bell's arguments lack convincing quantitative evidence to support the claim that there has been a transformation (Webster 1995) he avoids the crude "techno-evangilism" of other key commentators such as Alvin Toffler. Toffler (1970, 1980, 1990) describes western society as having gone through a radical

break with the past, evolving from an agrarian through an industrial to a "information society". Using little evidence beyond rhetoric, Toffler suggests that somehow the technology itself has forced a change, that can be seen as "a move to a better, more efficient, more just society" (Downey 1999: 122). Both Bell's and Toffler's work can be described as technologically determinist, in the sense that the influence of technology is stressed at the expense of the social. Furthermore, their work can be described as Utopian, since the technology is presented as providing a panacea for society's ills.

Castells (1996) reasons that an "information society" of sorts has been prevalent since medieval Europe's restructuring around scholasticism. While he recognises that in contemporary society certain economic changes are occurring which elevate the importance of information and the technological capacity to distribute it he maintains that social networks and identity remain as important as ever (Castells, 1998). While the arrival of an information age, centred on computers and telecommunication networks, has been long heralded Webster notes that it has failed to emerge. Indeed he argues that the claims that the UK has transformed into an "information society" are untenable when assessed using technological, economic, occupational, spatial or cultural criteria (Webster, 1995).

None of these works on "information society" are of direct relevance to this research. Yet indirectly they are important insofar as they highlight the tensions between academics that adopt a Utopian technologically determinist perspective and those who seek to empirically challenge it. Arguably, the lack of research into risks arising from Internet risk can be seen as a reflection of the dominance at the policy level of the former perspective. It is to writings on such policies issues that I now turn.

1.2 The Internet and policy issues

In this section I will briefly outline some of the sociological research on Internet related policy issues before focusing upon the writings of Selwyn, Moran-Ellis and Cooper, and Oswell. In particular the issues of the NGfL as a surveillance

tool (Selwyn, 2000), the simplistic construction of children in government NGfL policy documentation (Moran-Ellis and Cooper, 2000) and the conception of children as at-risk or dangerous (Oswell, 1998) will be addressed.

Internet related writings on policy issues have tended to deal with a broad range of topics. Thus sociological research has been undertaken on the democratising influence of the Internet (Carter, 1997; Poster, 1997; Kellner, 1999), social exclusion / inclusion with reference to citizenship (Ess, 1996; Steele, 1997; Keen et al, 1998; Downey, 1999) and on-line administration (Frissen, 1997). Research at a policy level has focused on various socio-legal issues, such as privacy (Elgesen, 1996; Denning 1997), on-line paedophile activity (Akdeniz, 1997), racial hatred (Whine, 1997) and cyber-crime (Thomas, 2000; Thomas & Loader, 2000). While all these works inform wider debate about the "net", research on Internet related education policy has frequently been more limited in scope, concentrating largely upon children and the NGfL. It is to this research that I now turn drawing upon the works of Selwyn, Moran-Ellis and Cooper, and Oswell.

Working within an empirically based critical tradition Neil Selwyn has provided a wide ranging evaluation of NGfL policy documentation and advertising literature. Arguing that the so-called "Learning Grid" is being constructed within a restrictive technocratic and economically determinist discourse Selwyn questions the societal, employment and educational rationales used to justify the introduction of the Internet into schools (1999a). Furthermore he draws attention to the confused messages surrounding the commercial presentation of the NGfL, which portray the technology as new but familiar, global yet local, technologically complex yet simple (Selwyn, 1999b). If, as Selwyn (1999a) argues, the NGfL is currently failing to meet the declared goals of cyber-democracy, employment provision and pedagogic reform then the question arises as to the actual outcomes of this initiative. In part these outcomes are unplanned and involve the creation of risks. This is an argument to which I will return in due course. Selwyn (2000) argues that one of the consequences of the "Learning Grid" is an increase in government surveillance capacity. Drawing upon the work of Foucault (1977) and Poster (1990), Selwyn highlights the surveillance capacity of on-line technology, arguing that "the NGfL has been, at least

partially, developed with a surveillance role in mind" (2000: 248). In particular Selwyn notes the "grid's" potential as a central conduit for school based performance data, the divulging of information when users register on the website and the potential to follow the electronic trails of site users (2000: 248-9). While this current research does not focus in particular, upon the "Learning Grid" this idea of surveillance is nevertheless important and one which provides useful insights when considering issues of control. Indeed this issue of surveillance and the Internet is addressed in detail in chapter eleven.

Drawing attention to the role played by NGfL documentation in convincing businesses of the benefits of helping to introduce the Internet into schools, Moran-Ellis and Cooper (2000) note that very little has been said about children and technology beyond the conventional construction of children as learners and future adults. Describing the NGfL documentation as economically deterministic, they observe that an unproblematic picture is painted of the relationship between the Internet and schools, in which the technology is presented as benign (Moran-Ellis and Cooper, 2000: para 2.4). It is argued that "if the Internet is identified as posing risks (in adult terms) to children ... [the] ... educational nature of the Internet becomes unstable" (Moran-Ellis and Cooper, 2000: para 2.4). Moran-Ellis and Cooper further note that the NGfL website carries a number of pages devoted to protecting children on-line and they speculate that the control of content on this website suggests an implicit knowledge of "other encounters" that children might have on-line (2000: para 2.4). While Moran-Ellis and Cooper introduce ideas of "risks" and "other encounters" the focus of their work shifts before they can elaborate upon the actual nature of these on-line dangers.

Focusing upon recent Internet policy discussions in the UK and Europe Oswell (1998) notes that three images of the child circulate in policy narratives on Internet content regulation. Namely the child as victim, the child-in-danger and the dangerous child. According to Oswell, "[t]he construction of the child-as-victim dominates discourse on child pornography and the Internet" (1998: 278). Thus the child-as-victim is associated with the activities of paedophiles, illegal images, and attempts at seduction through on-line conversations. The child-in-danger is constructed in terms of children accidentally accessing material of a

harmful nature. Harmful, in this context, can be defined in terms of "material that might affect their [children's] physical and / or mental development" (European Commission, 1996b: 6) Such material includes not only pornography or violent images, but also information promoting drugs, alcohol or even bomb making. According to Oswell (1998: 281) the key defining element of the child-in-danger is that the discovery of harmful material is accidental, unintended. In contrast, the "dangerous child" is constructed as intentionally seeking out harmful material. As Oswell notes "[w]hereas the child-in-danger is seen as passive and weak, the dangerous child is seen as active and aggressive" (1998: 281) This discourse of child-in-danger and dangerous child is not new but rather has a long genealogy dating back to the nineteenth century (Rose, 1985). Nevertheless, some uncertainty does exist as to who is actually at risk from the dangerous child. An insight is offered by Oswell's assertion that the dangerous child is "constructed predominantly as male. The young male is presented as a prototype of the violent, rapacious, criminal man" (1998: 281). This association with criminality links this concern with the safety of others, with the danger that the child poses to him or herself being at best a secondary consideration. The use of the three images at a policy level is criticised by Oswell as somewhat simplistic. While I agree with this assessment I would argue that these three images nevertheless provide the basis of a useful framework for considering the risks arising from school Internet use. Importantly this rhetoric allows for the idea that students are not only possible victims but also potential offenders. Students are not only "at risk" but are also possible of creating risk. I will return to this important point in the conclusion to this review on Internet focused sociological literature.

Overall, a range of sociological research has been undertaken at the policy level. Much of this work focuses on concerns that are not always directly relevant to schools. Within this broad category of writings I have focused upon on-line surveillance (Selwyn, 2000), risks to children (Moran-Ellis and Cooper, 2000) and the "dangerous child" (Oswell, 1998). These issues will inform subsequent debate about risks arising from school Internet use and hence I shall return to them in due course.

1.3 The Internet and identity

There has been a plethora of academic writings about on-line identities, focusing in particular on the idea of community. Yet little of this sociologically informed writing has addressed the issue of how school Internet access affects the identity of students and schools. Having drawn attention to some of the broader issues of on-line identity, I will focus upon Joo's (1999) discussion of cultural issues arising from Internet use in classrooms as well as Hesketh and Selwyn's (1999) article on the electronic reconstruction of school identities.

Surrounding the growth of Internet use in affluent western societies has been a body of broadly sociological work that has attempted to describe the impact of this technology on the social construction of identity. Research focusing upon on-line identity has dealt with such issues as the existence of virtual communities, (Rheingold, 1994; Wilbur, 1997; Foster, 1997; Watson, 1997; Jones, 1998; Baym, 1998) gender on-line (Plant, 1996; Adam and Green, 1998; Danet 1998), cyber-sexuality (MacRae, 1997; Shaw, 1997; Dietrich, 1997; Schofield-Clark, 1998) and the construction of ethnicity using the "net" (Mitra, 1997; Poster, 1998). Despite writings on "information poverty" (Holderness, 1998) and social exclusion (Haywood, 1998) a discussion of how socio-economic class might be constructed on-line is largely missing from this body of work. This possibly reflects that despite its increasing availability in the libraries and schools in economically developed countries, the "net" is largely an instrument of the affluent. Despite government and commercial literature stressing the range of people and places around the world that children will be able to access there is little research addressing the issue of how the Internet will affect children's identities. While research has been undertaken in educational settings on children, technology and identity often little is made of the context. For example, in an interesting article Lynn Schofield-Clark (1998) considers teen dating on the "net". While the research and much of the Internet use described takes place within a school setting, any specifically contextual issues that this raises are ignored. Two exceptions of this tendency to neglect the role of the school in Internet use and identity construction can be found in the work of Joo (1999) and Hesketh and Selwyn (1999).

Examining cultural issues in the classroom Joo argues that while the Internet offers novel opportunities to enhance teaching and learning by opening classrooms to the world it "does not eliminate cultural obstacles" (1999: 250). Rather cultural boundaries continue to exist on-line, such as the reliance on stereotypes and the use of culturally relative style, structure and content in web page design (Joo, 1999: 248-249). Furthermore Joo (1999) argues educational gains to be made from the experience of other cultural identities might be limited, as web content is strongly orientated towards dominant US values.

Focusing on institutional rather than personal identity Hesketh and Selwyn (1999) examine the electronic reconstruction of school identities using the World Wide Web. Noting that the Internet provides an opportunity for schools to market themselves they conclude that:

> Those schools who have the technological (and financial) capital to benefit from the information superhighway will continue to do so, whilst the majority of less-endowed schools will continue to be marginalised (Hesketh and Selwyn, 1999: 518).

Indeed a common theme of empirical research about on-line identity is the inescapable impact of the off-line world. Thus as Adam and Green argue while there exists an upsurge of interest in women experimenting with on-line identities, they face the "same old restrictions" of access to technology, limited time and lack of money (1998: 97).

In summary, there is little research that focuses upon school Internet use and identity. Yet insofar as Joo (1999), Hesketh and Selwyn (1999), and Adam and Green (1998) suggest that off-line cultural and economic boundaries continue to dominate on-line it could be argued that the school Internet might have little impact on students' identities. Nevertheless if school Internet use poses a risk to institutional identity and reputation, as I consider in chapter eight, then it is also important to recognise that it can also be used beneficially as a marketing tool (Hesketh and Selwyn, 1999). I shall now focus upon the literature that explores this issue of how the Internet is actually used in schools.

1.4 Institutional Internet use

Despite the introduction of the Internet into libraries, community centres and places of work, research on institutional Internet use tends to focus largely on schools. While I will mention in passing some of the numerous writings about effective use of the Internet I wish to focus mainly upon those pieces of research that deal with problematic issues arising from school Internet use. In particular I will concentrate upon the work of Lawson and Comber on school Internet censorship and the blurring of boundaries in schools. The justification for concentrating upon these two pieces of work is that they focus upon the possible dangers of the school Internet and will subsequently inform the analysis of on-line risks.

Writings considering school Internet use have largely concentrated upon "good practice". In particular government related bodies have funded and published a range of work covering planning (BECTa, 1996; BECTa, 1997a) purchasing (OFTEL, 1997) and good ICT management (BECTa, 1998). While some of these materials deal directly with the issues of censorship and security (SCET, 1996; BECTa 1997b; BECTa 1997c) they take the form of advice booklets with little or no empirical grounding. More notable research projects, such as that into the Superhighways Initiative (DfEE, 1997b), have focused upon good Internet practice while marginalising the issue of misuse. Other more academically informed research, casting varying degrees of light on the issue of good Internet practice, have also been undertaken (Selwyn, 1997; Selwyn, 1999c; Furlong et al, 2000; Russell and Russell 1999). While these studies are useful insofar as they inform pedagogic practice they largely ignore the potential negative outcomes of school Internet use. Indeed research considering the issue of on-line risks in schools is almost conspicuous by its absence. To an extent, the work of Lawson and Comber has attempted to address this lack.

Lawson and Comber (2000b) note that media attention on school Internet use tends to be focused upon the dangers of young people gaining access to pornographic or other material. While they label these concerns as an example of "moral panic", insofar as they can be seen as exaggerated and sensationalistic,

they nevertheless recognise that schools are still likely to be battlegrounds between those seeking censorship and those opposing it. While concern might focus upon students accessing unsuitable material, such as pornographic, bomb-making or hate engendering web-sites Lawson and Comber point out that a further worry in the schools in which they carried out their research was the access which undesirable others might have to students via electronic communication. Partially in response to such perceived threats, they argue that their fieldsite schools adapted a range of Internet control strategies. Namely restricting access to Internet machines, utilising filtering software, adopting Acceptable Use Policies, undertaking virtual surveillance and encouraging the use of an honour system (Lawson and Comber, 2000b). Ultimately Lawson and Comber's article on censorship and schools can be seen as important insofar as it highlights some possible on-line dangers while documenting school responses. In their conclusion, Lawson and Comber (2000b) remark upon the use by schools of Internet strategies that are "age appropriate". This suggests that not all students face, or even pose, the same on-line risks.

Drawing upon the influence of various writings on postmodernity Lawson and Comber (2000a) maintain that the introduction of the Internet into schools has the potential to blur certain boundaries. For example they draw attention to arguments that the use of computers creates a situation where the emphasis shifts from teacher-centred learning to a more student-centred approach, effectively blurring the boundaries between the traditional roles of teacher and student. Furthermore they note that the ability to work remotely through the information superhighway is likely to impact upon both home and the workplace in ways which may increasingly blur the boundary between work and leisure. The concept of blurring of boundaries is a useful one insofar as it highlights the potential of the Internet to confuse existing categories. This is an issue that I address in detail in chapter six.

Overall much of the sociological literature on Internet use in schools, is concerned with good practice and making effective educational use of the technology. Indeed, it might be expected that the first concern with any new technology should be to learn to utilise it efficiently. Yet, this in itself does not

justify the relative lack of research into the risks associated with school Internet use. It would be a mistake to believe that research into potential negative outcomes is of necessity negative in itself. Individuals seeking to benefit fully from a technology should also be aware of any risks.

In drawing conclusions from the sociological literature focusing upon the Internet, I will now highlight the importance of some of these issues for research into risk and the school Internet.

1.5. Conclusion: Key themes drawn from the sociology of the Internet

While any literature review unearths various items of interest, it is the ideas that subsequently relate to the research to which the researcher inevitably returns. Having considered the sociology of the Internet, with regard to technological narratives, policy issues, identity and institutional use I have touched upon some key themes that I now wish to briefly reconsider. Namely Oswell's descriptions of children as victim, in danger or dangerous, Lawson and Comber's argument that the Internet blurs boundaries and Selwyn's consideration of the surveillance potential of the NGfL.

While the initial categories of students "in danger" and as a "source of danger" emerged from analysis of the research data Oswell's article nevertheless provided inspiration in labelling and clarifying these categories. The three images of children, outlined by Oswell (1998), the child-as-victim, the child-in-danger and the dangerous child add an important dimension to any discussion of risk arising from school Internet use. Rather than defining students solely as being at risk the introduction of the concept of the dangerous child allows for the possibility that students pose a risk, creating danger for others. This distinction allows students to be perceived not merely as victims but also as potential offenders. This highlights that individuals are sources of risk as well as casualties of it. While the distinction between the child-as-victim and the child-in-danger is arguably important at a policy level I would maintain that this differentiation is of little concern in schools, where the posting of child pornography is much less of an issue than in wider society. Therefore, I would suggest that for this research it

would be practical to merge the two categories of child-as-victim and child-in-danger into one new classification that defines the child as being "at risk". This adequately allows for discussion of both the activities of paedophiles and harmful on-line content. As the research is situated within schools, I shall refer to this new category as the "student-at-risk". Although not seeking to change Oswell's (1998) description of the dangerous child I will also re-label this category as the "dangerous student".

Thus, the "student-at-risk" can be perceived as being physically or mentally in danger from the on-line activities of paedophiles, or the accidental accessing of illegal and harmful material on the net. Arguably this is in contrast to the "dangerous student", who poses a risk to other's reputation, security or finances through his / her on-line activities. Importantly this is not to suggest that these two categories are exclusive, obviously at various times the student can be at risk and / or dangerous. Rather I would argue that individuals interpreting certain incidents would tend to privilege one category above the other depending on the situation. Furthermore as these two categories are not contradictory it is not problematic if individuals define the students as being at risk and dangerous simultaneously. These conceptions of the "student-at-risk" and the "dangerous student" will prove central to this thesis providing useful insights when describing staff / student narratives and school responses to Internet risk.

Perceptions of student intentions and possible on-line hazards might vary depending on age. As already noted Lawson and Comber (2000b) remark upon the importance of "age appropriate strategies". Indeed the idea that primary school children might be seen as broadly at risk, while older secondary school children with more life experience might be perceived as mischievous and therefore dangerous is not a radical one. The age of the student is an important variable that I shall return to when interpreting the research data.

The concepts of blurred boundaries and surveillance are of significance as they are each the focus of subsequent chapters.

Lawson and Comber (2000a) note the potential for the Internet to blur certain boundaries. Drawing upon this idea in chapter six I argue that the recontextualisation of certain material on the web has led to interpretative difficulties with regards to pornography, hate engendering sites, websites encouraging experimentation and copyright.

While Selwyn (2000) focuses upon the surveillance capacity of the NGfL, he nevertheless provides some insights into the observational capacity of the Internet. Thus he notes that a precedent for recognising surveillance as a form of control can be found in the writings of Foucault (1977) and Poster (1990). Surveillance can be seen as a form of control, insofar as it is an attempt to impose social order and accountability (Ball, 2000). The issue of controlling Internet use through surveillance is addressed in chapter eleven.

Having highlighted concepts from the sociology of the Internet which have informed this research and form the basis of subsequent chapters I will now turn my attention to the literature on the sociology of risk.

2. The Sociology of risk

There is no sociological literature on risk that deals directly with Internet use. Nevertheless, a consideration of the broader literature on risk will highlight some key concepts that provided insights when analysing the data gathered from the fieldwork sites.

Before considering various sociological perspectives on risk, a distinction needs to be made between realism and social constructionism. This will allow me to situate the schools of thought on risk within a wider discourse and enable a consideration of the fundamental nature of risk. Following this consideration of realist and social constructionist interpretations of risk I will focus upon the three broad sociological / anthropological approaches to risk evident in the literature. Namely, the discourse analysis approach, which draws on the writings of Foucault, the "risk society" perspective, which owes much to the work of Beck and Giddens stressing the processes of globalisation as well as

individualisation, and the cultural approach, found in the work of Douglas and Wynne. A review of the literature representing all three schools of thought will highlight the benefits and pitfalls of the various attempts to interpret and evaluate risk. While it is the third of these approaches to risk analysis which I adopted in interpreting the data, a consideration of writings on risk discourse and "risk society" should provide a deeper understanding of the arguments presented from the cultural perspective. In drawing upon the ideas central to the cultural approach I focus in particular upon actual / perceived risks and the role of expert / layperson knowledge. These themes are considered in detail in the conclusion to this section on the sociology of risk.

Prior to considering the three broad sociological schools of thought on risk, I will seek to draw a distinction between realist and social constructionist viewpoints. This will provide an opportunity to differentiate between those risks that are merely perceived and those that are actual.

2.1 Situating sociological approaches to risk

In social science literature the phenomenon of risk tends to be situated somewhere in or between the realist / social constructionist perspectives. The realist approach, which emerged from such disciplines as engineering, statistics, psychology, epidemiology and economics, treats risk calculations as "objective facts" or "absolute truths" (Bradbury, 1989: 382). Consequently from this perspective risks can be "identified through scientific measurement and calculation and controlled using this knowledge" (Lupton, 1999: 18). Drawing upon the fields of social anthropology, sociology, social geography and cultural studies the social constructionist risk perspective emphasises the aspects that realist approaches are accused of neglecting, namely, the social and cultural contexts within which risks are understood and negotiated. From this perspective, all knowledge about risks is bound to the socio-cultural contexts in which it is generated. According to this approach as knowledge is never value free but always a product of a way of seeing, debates about risks always involve questions of cultural representation, meaning and political position.

While risk discourse analysis occupies a strong social constructionist position, focusing on how people construct risk narratives, both "risk society" and cultural approaches combine differing degrees of realism and constructionism. In combining social constructionist and realist viewpoints, the "risk society" and cultural approaches allow for both a consideration of individual risk perceptions as well as some objective assessment of the risks. This in turn allows a distinction to be made between actual and perceived risks.

Actual risk are those which have an existence in the physical world insofar as they have come to pass. Examples of actual risks include cancer from smoking tobacco, death from AIDs and illness from nuclear pollution. Perceived risks exist solely in the social world, they are wholly constructed through discourse. Examples of perceived risks are politically extremist conceptions of the hazards of inter-racial breeding or fear of abduction by extra-terrestrials. To ignore perceived risks is to impoverish any attempts to fully understand individuals' risk perceptions and responses. Being able to distinguish between actual and perceived risks is of importance for this research in that it allows a distinction to be made between ungrounded fears and real dangers. I shall return to this point in the conclusion to this section on the sociology of risk.

Having situated the three main sociological approaches to risk within the wider narrative of realism and constructionism I will now turn my attention to risk discourse, "risk society" and the cultural perspectives in turn. Having drawn out the lessons to be learnt from each approach I will then expand upon some key concepts from the cultural approach to risk.

2.2 Risk discourse analysis

The analysis of risk that focuses solely upon discourse is often ignored in the broader risk literature (e.g. Caplan, 2000). A reason for this neglect is that in concentrating purely upon discourse the threat posed by actual dangers, such as pollution, AIDs or natural disasters, is ignored. Rather researchers in this tradition are interested in how risk discourses are used as instruments of social

control. In expanding upon this point, I will briefly consider the influence of Foucault, plus some contemporary concerns and criticisms of this approach.

Writings focusing upon risk discourse draw heavily upon the work of Foucault, adopting a very strong social constructionist position. While Michel Foucault did not dwell specifically upon the topic of risk in his writings, much of what he had to say on government and modernity has been applied by scholars, such as Castel (1991), to the analysis of risk as a socio-cultural phenomenon. An important insight offered by Foucauldian perspectives on risk are the ways in which the discourses, strategies, practices and institutions around a phenomenon such as risk bring it into being and serve to construct it (Lupton. 1999: 84). It is argued that only through these discourses, strategies, practices and institutions is risk known. For advocates of this approach the nature of risk itself is not the important question for analysis. Rather risk is seen as a "calculative rationality", not as a thing in itself (Dean, 1999).

Drawing on Foucault's (1991) writings on mass surveillance, monitoring, and observation, risk can be constructed as a disciplinary, moral technology. Thus in late modern societies to not engage in risk avoiding behaviour is considered "a failure of the self to take care of itself - a form of irrationality, or simply a lack of skilfulness" (Greco, 1993: 361). As expert knowledge about risk has proliferated in late modernity, the various strategies which individuals are required to practice upon themselves to avoid risk have equally proliferated. For example, pregnant women are positioned in a web of surveillance, monitoring, measurement and expert advice that requires constant work. Indeed in the United States women have been prosecuted and imprisoned for "foetal endangerment" by refusing to take medical advice or give up certain drugs (Handwerker, 1994). Bauman (1993) argues that strategies dumping risk-avoidance behaviour on the individual help to create an enormous market in risk avoiding devices, from vitamins to video-surveillance systems. In this sense risk-avoidance is not so much a "chance for the future" as a way of maintaining a billion-dollar industry.

This Foucauldian influenced approach is useful, insofar as it draws attention to discourse as an instrument of control and introduces the idea that risk perceptions

might encourage self-policing. Yet this perspective ignores the existence of actual danger. Ultimately this limits the value of this approach in any work that is focused upon assessing risk. With this in mind, I now turn my attention to the writings on "risk society".

2.3 The "risk society" approach

The "risk society" approach can be seen as wavering between a realist and a weak social constructionist position. Its exponents consider the politics, macro-level meanings and strategies of risk, focusing upon such processes as individualisation, reflexivity and globalisation which are perceived as converging in the "risk society" of Western nations (Lupton, 1999: 58). In considering this perspective, I shall briefly contemplate the writings on risk of Ulrich Beck and Anthony Giddens, before focusing on the key issues of globalisation and individualisation. Finally, I will examine some criticisms of this approach.

Ulrich Beck's book *Risk Society*, published in Germany in 1986 and translated into English in 1992, has been enormously influential (Caplan, 1999: 2). Beck argues that there has been a shift from classical industrial society to a new self-endangering modernity, that is a "risk society". In subsequent writings (1994, 1995, 1996a, 1996b, 1995 with Beck-Gernsheim) he expands upon this argument that the nature of contemporary risk, which he sees as qualitatively different from its historical predecessor, has become a defining feature of modern society. Like Beck, Giddens (1991, 1994, 1998) sees the world today as having entered a new phase of "late modernity", which he sees as an inherently risk obsessed culture. For Giddens, the concept of risk is "fundamental to the way both lay actors and technical specialists organise the social world" (1991: 3). The work of Beck and Giddens has many other similarities; in particular they both argue that the processes of globalisation and individualisation are key features of this "risk society".

The idea of globalisation is central to the writings of Beck and Giddens on risk insofar as they both maintain that the dangers which society now faces are global ones. They argue that contemporary risks exist on an international scale (e.g. the

spread of Foot and Mouth disease, the explosion at Chernobyl Nuclear Power Station) with consequences that can spread across future generations (e.g. AIDs).

In addition to the globalisation of risks Beck and Giddens both argue that there has been a shift in the relationship between the individual and society, with old social categories of modernity, such as class, losing much of their salience. They contend that a disintegration of these "old certainties" and the compulsion to find and invent new ones leads to individualisation. This erosion of "old certainties" fosters freedom to choose, but is also fraught with risk (Beck and Beck-Gernsheim, 1995). Consequently rather than relying on socially prescribed biographies individuals now seek to produce their own through a process of reflexivity (Beck, 1992: 135). Furthermore this reflexivity gives rise to an unwillingness to accept the truth claims of scientific knowledge (Beck, 1992: 157). Faced with risks and growing uncertainty the search for morality shifts either to individual effort, notably based around the body, with exercise and dietary regimes, or to social and environmental movements (Caplan 2000: 7).

Although Beck and Giddens' writings on risks provide a powerful description of recent social change, they have also been the subjects of criticism. While as Wynne (1996: 46) notes, both Beck and Giddens have started to consider social actors, their early work has been criticised for largely ignoring the social and cultural aspects of risk (Lash, 1994; Day, 2000). Indeed in initial writings both Beck and Giddens largely ignored the importance of non-expert apprehensions and lay-responses to expert systems, rather leaning towards a strongly realist viewpoint.

Furthermore, the "risk society" approach has been criticised for relying heavily on rhetoric, while being too speculative in making broad and loose conjectures. Indeed it is notable that attempts to apply this theoretical framework to research seem somewhat inconclusive, failing to make connections between research data and the macro-level arguments of Beck and Giddens (e.g. Furlong and Cartmel, 1997). Of course this is not to deny that Beck and Giddens make a highly influential contribution to sociological debates about risk. However, in my own

research I gained more constructive insights from employing the cultural perspective on risk.

2.4 The cultural approach to risk

While some authors within the cultural approach to risk adopt a position towards the strong end of constructivism, for example Douglas, others, such as Wynne, combine elements of both realist and social constructionist viewpoints. I will consider the work of both of these writers, before drawing out some key themes which informed my research.

Over a period of many years, the anthropologist Mary Douglas has written extensively on risk, co-authoring a volume with Aaron Wildavsky in 1982, before writing two solo works on risk acceptability (1985) and blame (1992). She argues that risk is always social and that it can be seen as a contemporary western strategy for dealing with danger and "otherness". Indeed Douglas suggests that the "other" is a key concept in risk formation. Often perceived as threatening, the "other" results in the creation of boundaries between inside and outside the body / society. It is at these margins of the body / society that concerns and anxieties about purity and danger are directed.

While Douglas's work provides a persuasive critique of the realist approaches, emphasising that risk judgements are political, moral and aesthetic, it has been criticised for reducing real dangers to little more than metaphor, trivialising real hazards and "eliminating danger altogether" (Kaprow, 1985; 347). Her writings are frequently re-interpreted as implying that lay perceptions of risk involve inaccuracies and errors of judgement because of the contaminating influence of cultural and social processes.

Working within a broadly cultural perspective on risk Wynne (1989, 1996) attempts to directly address the two issues of assessing actual risks, whilst interpreting expert / lay person knowledge. Wynne argues that in order to assess actual risk the perceptions and responses of scientific experts and lay-people need to be understood on a hermeneutic level. For example whilst studying

claims that the herbicide 2, 4, 5-T was harmful to farm workers in Cumbria, Wynne (1989) noted that scientists who claimed that the product was not hazardous if properly used, ignored the fact that because of the contingencies of work, it was rarely prepared and used according to the safety instructions.

In conclusion it should be recognised that writers adopting cultural approach to risk do not seek to privilege the experiential truth of lay actors over the prepositional truth of experts. This would merely invert the existing scientific knowledge hierarchies (Szerszynski et al, 1996: 7). Rather the concern is to understand, interpret and assess risks from a hermeneutic perspective. Hermeneutic in this sense can be seen as "a way of understanding action within the larger framework of the world-view which produced it" (Lawson & Garrod, 1996:118). I shall now draw out some of the key arguments from the cultural approach to risk that have informed my research into dangers arising from school Internet use.

2.5 Conclusions: Key themes drawn from the sociology of risk

Having considered realist / social constructionist viewpoints and some key writings on the sociology of risk I will now examine several important themes which can be drawn from the literature adopting the cultural approach to risk analysis. Thus I shall expand upon the importance of actual and perceived risks as well as the role of expert / layperson knowledge.

Drawing upon the cultural approach I argue that how actual risks are selected, perceived and addressed is a function of the social. While merely perceived risks are not directly related to danger in the physical world, they can affect people's behaviour and their study can nevertheless provide insight into social processes. In attempting to assess whether a risk in this research was actual or perceived, I consider whether the threatened hazard has come to pass either in the school or in the wider world.

To suggest that the position of expert or layperson naturally corresponds with a particular level of risk knowledge in contemporary society is problematic. Actors

from both positions are capable of illustrating ignorance about risks. A more useful distinction than expert / layperson knowledge is to consider the depth of reflexive experience and informed research. Thus, it should be recognised that expertise in the chemical industry does not necessarily equate with a comprehensive knowledge of the risks faced in people's everyday lives. Neither does practical experience of these risks mean that people understand the real nature of the dangers they face. Rather what is required is a hermeneutic approach that combines knowledge at the technical level with understanding arising from experience.

In summary it should be noted that in considering realist / social constructionist perspectives and the varied approaches to the sociology of risk I have highlighted the distinction between actual and perceived risks as well as the need to understand both expert and layperson perspectives. In concluding this chapter I will seek to provide an overview of the insights from both the Internet and risk literature, before drawing together threads which span the writings in both of these fields.

Conclusion

While it has been noted that there is no literature which directly addresses the issue of risks arising from school Internet use I have argued that a review of the sociological literature on both the Internet and risk provides some relevant insights. Drawing upon the Internet literature I noted that Oswell's distinction between the child at risk and as a source of danger, Lawson and Comber's assertion that the Internet blurs boundaries and Selwyn's description of the NGfL as a surveillance tool have all informed this research. Furthermore drawing on the cultural risk perspective I have noted the importance of distinguishing between actual and perceived risk and the necessity of reflexively examining both expert and layperson risk knowledge. In conclusion, I will argue that four main assertions regarding school Internet use should be drawn. Namely, that both staff and student risk perceptions must be analysed, that the question of who is actually at risk from the Internet needs to be addressed, that a distinction needs to

be made between actual and perceived risks, and finally that school attempts to alleviate Internet risks should be described.

If risk perceptions are to be fully understood in schools then both staff and student narratives must be considered. Indeed these particular narratives form the focus of chapters four and five respectively. It is recognised that another key party in constructing a narrative of Internet risks is the government, so where pertinent I have given voice to the views embodied in the various documents on the NGfL and Internet safety. Additionally I have made reference to on-line incidents as reported in the mass media where I have felt that it is appropriate. While a case might be made for including the views of LEA officials, school governors or parents in this research this was not possible due to the limits of time. Nevertheless, I received no indication during my fieldwork that the inclusion of such parties would alter my findings.

In describing risks, it is important to identify who is actually in danger. Thus drawing upon the narratives of the "student-at-risk" / "dangerous student" I have sought to draw a distinction between students considered to be at risk and those considered to be a source of danger. I have suggested that the age of the student might be an important factor in making such distinctions. Due to the limits of time and a lack of evident concern in schools, narratives focusing upon the staff at risk and the dangerous employee are considered merely in passing.

Having considered various risk narratives, I argue that there is a need to make some assessment about the likelihood of these dangers occurring. Drawing upon incidents in school and wider society distinctions can be made between actual and perceived risks. In assessing the risks arising from school Internet use I focus upon the "student-at-risk" in chapter seven and the "dangerous student" in chapter eight. In addition to assessing whether risks are actual, I attempt to make some observations regarding the frequency of their occurrence.

Finally, individuals often seek knowledge about risks so that they can take suitable precautions to avoid possible dangers. I argue that a consideration of the attempts made by schools to control "net" use adds to an overall understanding of

school Internet risk. In describing such attempts at control I focus upon institutional rhetoric in chapter nine, exclusion of unsuitable material and "dangerous students" in chapter ten and surveillance in chapter eleven.

In the first two chapters, I have considered the rationale for this research and the relevant sociological literature. To complete this description of the research background I shall concentrate on research methods and issues in the following chapter. I will outline the research focus before describing the sampling techniques used and providing a brief sketch of each of the fieldsites. Having considered the different research methods utilised and the process of data analysis I will then discuss the ethical issues that arose.

Chapter Three

Research focus and methods

Introduction

Computer mediated communication, such as the Internet, has moved rapidly from the status of futuristic dream to exponentially exploding reality (Ess, 1996: 1). In the previous two chapters I have sought to provide a rationale for this research and review relevant academic writings. I concluded the previous chapter by making four assertions that are relevant to this research. Namely that there is a need to understand both staff and student risk perspectives, that the issue of who is at risk needs to be addressed, that an assessment of whether risks are actual or perceived should be made and that school attempts to alleviate risks should be described. This chapter is concerned with the research focus, sampling techniques, research methods, data analysis and ethical problems that arose from the research.

In elaborating upon the research focus I consider questions relating to the dangers that staff and students saw in Internet use, the reality of these hazards and the precautions taken to avoid them. Additionally I review some questions, which although important, did not directly fit in with the developing research focus. Following on from this I outline the sampling techniques, describing how schools were chosen for this research and how individuals as well as locations were selected within these institutions. In this section I also provide a brief sketch of all eight schools in which the research was carried out. I then consider the research methods that were adopted, discussing the processes of observation, interviewing and content analysis, before focusing on the process of data analysis. Finally, I note that two main ethical problems emerged relating to the asking of questions about potentially embarrassing subjects and the witnessing of student abuse of the school Internet.

1. Research focus

The focus of this research was the risks arising from Internet provision in eight schools. I was interested in staff and students' views of the possible dangers arising from the school Internet. While I was aware of a public narrative evident in the mass media that constructed the Internet as a "playground for paedophiles" and a "library of porn" I was concerned with the viewpoints of individuals who worked and studied within educational institutions. Furthermore, I wanted to discover whether perceptions of the Internet as dangerous invoked the narrative of the student as victim or as a source of peril. That is, whether individuals were concerned about the risk of students accessing on-line pornography because they believed the child might suffer mentally or rather were they anxious about the impact that such incidents might have on the reputation of the school. I was also aware that certain concepts such as suitability, pornography and racism were constructed through complex social processes and I was curious as to whether such complexities would lead to differing interpretations of on-line incidents in schools. In addition to describing these staff and student risk perceptions I was keen to assess whether these feared incidents had actually occurred in the schools studied or in wider society. Indeed I wanted to know what Internet related "incidents" had occurred in schools and how they had been dealt with.

Beyond a concern with risk perceptions and assessment I also wanted to explore school attempts to alleviate dangers and control Internet use. Thus questions arose relating to the role of rhetoric in controlling "net" usage, the forms of surveillance of on-line students, the regulation of physical access to networked computers and the punishments for Internet misuse. Furthermore anticipating that schools would seek to regulate Internet use I wanted to know how students responded to such attempts at control. Would they be apathetic, avoid the Internet or develop strategies to evade punishment for Internet misuse? If students did seek to resist staff attempts to control Internet use then I was curious as to what forms these resistance strategies took.

In seeking to describe and assess risk perceptions and responses I was concerned with issues of danger, that is, hazards that posed a physical or mental threat. In

this sense, I was not interested in the impact on schoolwork of recreational Internet use or of the difficulty of finding suitable educational on-line material. Prior to the research, I recognised that websites that featured information that was incorrect or pitched at the wrong academic level for students might represent an educational problem. Yet I believed that to actually describe them as a risk would be using the concept in a far too liberal sense. Similarly, I felt that focusing upon lesser issues, such as on-line swearing, would divert me from my main concerns.

In summary my main focus was staff and student perceptions of the risks arising from school Internet provision. In addition I was concerned with assessing whether these risks could be labelled as actual or perceived. Additionally I was interested in attempts by staff to control student Internet use and the responses such endeavours created. Although I recognised that from an educational point of view issues such as students using the Internet to play when they should be studying or the difficulty of finding useful websites were significant, I maintained that they did not represent actual danger. Indeed the failure of any respondents to use the language of risk to describe these problems supported this assertion. Having outlined the focus of this research I will now describe how I chose my field sites and provide brief sketches of the schools in which my research was based.

2. The case studies

A case study can be defined as the "development of detailed, intensive knowledge about a single case or a small number of related cases" (Robson, 1993: 89). Typically, case studies involve the selection of a small number of situations, individuals or groups of interest, the study of these cases in their context and the collection of information via a range of data collection techniques including observation, interviews and content analysis.

In total, I selected eight institutions as case studies. For brief details of the research fieldsites please see table 1 over the page. As I was focusing upon school Internet use all of these institutions were educational and all had Internet

Table 1

Details of the research fieldsites

Name of School	Age Range	Number of Students (Approximately)	Months School On-line (Prior to Research)
Avenue	Primary	80	24
Brooklands	Primary	90	24
Canalside	Secondary (11-16)	400	12
Dalehouse	Secondary (11-16)	800	12
Eastway	Secondary (11-18)	900	Gained widespread Internet access during research *
Forestfields	Secondary (11-18)	800	36
Greenswold	Secondary (11-18)	1, 000	18
Hightree	Post-16	900	Gained Internet access during research

* Prior to the start of the research Eastway Secondary School had one Internet machine in the library that allowed the school ten hours free access to the web per week.

provision. Additionally all eight schools were co-educational and situated in the north east of England. These last two factors did not reflect a conscious sampling choice but rather arose from the difficulty of accessing single sex schools and the impracticality of selecting case studies spread over a geographically wide area. The schools I chose differed with regards to student numbers, the age range of students, the extent of ICT provision and the period during which they had gained Internet access. Furthermore, the schools were located in various rural, suburban and urban areas. I will consider the extent to which these similarities and differences reflected sampling decisions as I describe the process through which these schools were selected as case studies.

In the initial stages of the research six schools, all post-primary, were contacted by letter with a view to participating in a study focused on ICT. Three schools, Hightree, a post 16 institution, Eastway and Forestfields, both 11-18 establishments, responded positively and the fieldwork started in the spring of 1999. All of the six schools had been chosen from an extensive list of secondary schools involved in teacher training in the region. While it was not possible to ascertain why the three remaining schools did not respond, a follow up enquiry to one of the schools revealed that the Vice-Principal believed the school's ICT provision was too insubstantial to warrant research, and while expansion was planned research would not be welcomed until the staff and students had become "acclimatised" to the new technology.

Once the research focus began to emerge it was decided to expand the sample. Drawing upon the ideas of Glaser and Strauss (1967) concerning theoretical sampling I felt that subsequent fieldsites should be selected where possible to produce a diversity of categories and information. Furthermore I recognised that findings that emerge from the study of heterogeneous sites are more robust and more likely to be useful in understanding other sites than ones emerging from the study of several similar sites (Schofield, 1993; Kennedy, 1979).

Hence primary schools, 11-16 and 11-18 institutions were approached (it was felt that one post sixteen institution was sufficient considering the scale of the research). This allowed for a sampling of students by both age and type of

educational institution. Additionally an effort was made to approach schools that had established Internet use and those institutions where the Internet had been recently introduced. This represented an attempt to generate diverse data and allow for the possibility that risk perceptions might change in schools as staff and students gained more on-line experience. I was also conscious that situating the research in institutions with differing levels of ICT provision might generate information that was more diverse. Other factors I took into account when selecting schools were the size of the student population and the location of the institutions. Thus, I selected schools in urban, suburban and rural areas. Finally, I was aware that that in selecting case studies I should take into account broad issues of diversity relating to socio-economic class, ethnicity and gender.

The Heads of fourteen schools were sent a letter explaining the focus of the research and asked if they would consent to take part. Six replied positively. While attempts to discover the reason for non-response failed to produce any information at that time, the Head of one primary school in the research subsequently remarked that the unresponsiveness might reflect that many secondary schools were only just acquiring Internet access.

Of the six schools that responded to the second wave of letters, one, an 11-18 institution, was later dropped from the sample after repeated difficulties in arranging an initial visit. The final sample was made up of the three institutions that had provided the initial fieldsites in addition to a further five schools, Greenswold another 11-18 institution, Dalehouse and Canalside, both 11-16 establishments, and Brooklands and Avenue, which were both primary schools.

I felt it was important to undertake multi-site studies to generate a more diverse range of information, provide a firmer basis for generalisation, and avoid what Firestone and Herriot (1984) labelled as the "radical particularism" of many case studies. Yet a danger existed in undertaking multi-site studies that the larger the number of sites, the less intensive and prolonged the research in each case (Schofield, 1993; Firestone and Herriot, 1984). However this only becomes problematic when it threatens the internal validity of the study. That is, when the amount of research carried out at a particular site is insufficient to provide

accurate findings. In this case, the amount of research carried out at each fieldsite school enabled accurate and valid data to be gathered. While the time spent observing students' Internet use and carrying out interviews at both of the primary schools was markedly less than in the other six schools this was felt to be appropriate. Since both schools had fewer than 100 students and only four full-time teachers, less time was necessary for the relevant information to be gathered. I would argue that an accurate picture of perceptions about the Internet and its use was constructed in both cases. The exact time spent in each school is discussed below.

Consideration of sampling is not limited to the selection of fieldsites for investigation, but is often equally important within cases (Hammersley and Atkinson, 1995). Where cases are not sufficiently small to be subjected to exhaustive investigation, decisions need to be made about where as well as when to observe, who to interview, what to record and how. Accordingly three major dimensions along which sampling within cases exists can be identified: time, people and context (Hammersley and Atkinson, 1995).

It was recognised early in the research that use of the school Internet might fluctuate depending upon the time of the day. While sixth form students could use the Internet during free periods, other students were largely restricted to making personal use of the Internet either outside school hours or during breaks. Thus observations were carried out at various times of the day, during lesson time, before and after school as well as during breaks. At Forestfields in particular it was noted that students tended to use the Internet for prohibited activities after the end of the school day when they were no longer supervised by staff. In this particular case the day of the week was also an important factor in observing Internet use. After school on Fridays Internet use in the Learning Resource Centre (LRC) at Forestfields was unsupervised by either staff or student monitors. Additionally it was felt important to carry out research over the course of at least one school year to allow for changes brought about by fixed events in the school calendar, such as the approach of the Christmas holidays and the summer exams, and to gather information on how perceptions and Internet use changed over time.

No research situation will prove socially homogenous, and the adequate representation of the people involved in a particular case will normally require sampling (Hammersley and Atkinson, 1995). It was decided that it would only be necessary to allow for sampling of those variables that academic literature, initial research and intuition suggested might be important in constructing a valid representation. Thus, I was aware that the sampling should take account of differences in socio-economic background, gender, ethnicity and age. Additionally I focused upon the individuals' institutional role and their degree of involvement with the Internet. These sampling issues are discussed in more detail below.

The first points of contact in all schools were the Heads who were sent letters asking whether they would be willing to take part in the research. In all the schools, except Brooklands, this request was then passed on to the individual with the responsibility for school Internet use. In Avenue, Dalehouse and Forestfields this was the ICT co-ordinators, at Canalside and Eastway, the Head of the Information Technology (IT) departments, and at Greenswold and Hightree the ICT managers. At Brooklands the Head, who declared a keen personal interest in school based research into ICT use, arranged initial interviews and observations himself. This first contact with staff responsible for the school Internet generated much information. However, to allow for the sampling of a full range of perceptions the research sample was expanded to include staff less involved with Internet provision.

Initial contact with students had often tended to focus on those who used the Internet extensively. As the research progressed attempts were made to include less frequent "net" users. Furthermore I recognised that students were subject to different expectations and time restrictions relating to Internet use. For example, students studying for General National Vocational Qualifications (GNVQs) had large amounts of time during which they were expected to gather information from, amongst other sources, the World Wide Web.

I also sought to include in the research both individuals who used the new technology on an almost daily basis, and those who rarely, if ever, used it.

Additionally I considered that gender might be an important variable in this research, so the sampling took account of this belief. However, no conclusive evidence was gathered to support this view.

Overall within the eight schools attempts were made to observe and interview staff who had distinctly differing roles, students taking academic and vocational courses, frequent as well as infrequent "net" users and a representative sample of both males and females.

Linked to this attempt to include a representative sample of people in the research was an awareness of the importance of context, and in particular location. While students keen to use information communication technology congregated in locations where the Internet was situated, an effort was made to visit other locations, such as non-technical subject areas and student bases to interview students found there. Yet as observation of Internet use was a central part of the research much time was spent in the main Internet open access areas, which were the Learning Resource Centres at Dalehouse, Forestfields, Greenswold, and Hightree, and the dedicated IT suites at Canalside and Eastway. In both primary schools Internet access was not concentrated but spread evenly throughout the classrooms, with a few machines in each. Additionally I observed Internet use in peripheral areas, such as Sixth form bases and subject areas. A key feature of Internet access in the sixth form bases at Eastway, Forestfields and Greenswold was the relative lack of staff supervision. As I recognised that students' use of the Internet might differ between lessons and other times, I observed on-line activities both in lessons as well as outside of them in all eight institutions. Lastly, the staff rooms presented good areas for making contact and gathering information (Woods, 1979: Hammersley, 1980).

Having considered the case studies chosen I will now provide a brief sketch of each of the eight educational institutions used in the research.

2.1 Description of research fieldsites

Eight schools were used as fieldsites. Two of the institutions were primary schools, five were secondary schools and one was a post-16 educational establishment. Of the five secondary schools two were 11-16 institutions while the remaining three schools all had sixth form provision.

2.1.a Primary schools

Avenue was a rural village primary school that had gone on-line two years before the start of the research. It had four full-time staff, two of whom, the head and ICT co-ordinator, were highly committed to school "net" use. While the head was involved in ICT consultative committees at the local government level, the ICT co-ordinator, Ella spent a day each week on release helping at Forestfields secondary school. School numbers were small, just over 80 students, but each classroom had at least two computers with Internet connection.

Brooklands primary school had received NGfL money at roughly the same time as Avenue and so also had gone on-line two years prior to the start of the research. A rural village school with just over 90 students, it too was well provisioned with ICT. All three classrooms had four Internet linked machines and in addition the school had twenty "Dreamwriter" lap top computers so that the pupils could learn to use a keyboard. The head, Cliff, an ICT enthusiast, declared himself a "disciple of Papert" with a keen interest in "giving powerful computers to young children" (Cliff, Head, Brooklands). Of the remaining three full time staff, Jo, the ICT co-ordinator had training in the use of ICT in education. The school was involved in a European joint writing project that relied heavily upon e-mail use.

2.1.b Secondary schools

Canalside was an 11-16 school with over 400 Students. The school had gained Internet access a year before the start of the research, and had three main computer suites with 60 plus Internet machines. The IT department had

responsibility for school "net" provision and the Head of IT, Wilf, was responsible for general ICT provision and training. During the research period the school management considered and rejected the possibility of using ICT facilities, such as electronic white boards and webcams, to access classes at nearby Greenswold.

Dalehouse, an 11-16 institution with around 800 pupils had gained Internet access a year before the research started. The ICT manager was a geography teacher with a keenness for technology. The school had a main suite of over 30 Internet linked computers in the library, with an additional suite with 20 on-line machines used mainly for business studies. The school actively encouraged Internet use, allowing a wide range of recreational activities. Indeed towards the end of the research plans were being drawn up to turn the library into an after school cyber-cafe, open to parents and students alike.

At the start of the research **Eastway** had a single on-line machine situated in the library. An 11-18 institution with 900 plus students, it subsequently went through an extensive program of installing over eighty on-line machines. These Internet machines were mainly situated in three areas, namely in the IT department, a dedicated business studies suite and in a general access computer suite adjoining the library. Additionally a few Internet computers were situated in the sixth form base. The person with responsibility for ICT provision in the school was the Head of the IT department.

Forestfields, was an 11-18 school that had gone on-line three years prior to the start of my research. While Internet access for its 800 plus students was located in the Learning Resource Centre and the sixth form room, there were a further two large classroom suites used for computer studies and business courses. While these last two rooms each had over twenty Internet linked machines, there were only twelve situated in the LRC and five in the sixth form room. In addition to regular lessons the school also ran a wide range of computer based night classes. The ICT co-ordinator was also head of the IT department.

Greenswold, an 11-18 school with almost 1,000 students, had enjoyed Internet access for eighteen months. While there were only eight Internet machines in the library and three in the sixth form base, on-line provision was being expanded through the addition of over a hundred machines based in three main computer suites. In the year the research started the ICT co-ordinator, a science teacher, became a full time ICT manager, with responsibility not only for Internet provision in Greenswold but also in a cluster of local primary schools. Indeed the network at Greenswold served as a hub through which local primary schools could access the Internet. Amongst other initiatives, the school introduced a Cyber-dad program where students and their fathers could attend Saturday morning training sessions and learn how to use the Internet.

2.1.c Post-16 institution

Hightree, a post-16 institution with over 900 students had no Internet access prior to the start of the research. However, within a year of the research starting they had introduced an Internet suite with thirty-two computers linked to the web. A further nine on-line machines were situated in the adjoining library and another forty plus machines were located in two dedicated computer studies suites. Although there was the potential for all thirty-two machines in the Internet suite adjoining the library to be on-line, it was decided by the school management that Internet software would only be installed on sixteen of the machines. According to Tony, the ICT manager, this was to free up machines for word processing or other off-line activities and to avoid turning the room into a cyber-cafe. Responsibility for maintaining the network fell to Tony, the ICT manager, who had been recruited from the computing industry. As a full-time systems specialist his input into the running of the system was greater than that of the Head of science, who had responsibility for funding, or the ICT co-ordinator.

2.1.d Typicality of the research fieldsites

While I would argue that the data gathered in the two primary schools potentially provides an indication of staff / student attitudes in other primary schools towards Internet use some care needs to be taken in using this information. The two

primary schools included in my research both had fewer than a hundred students and were situated in small rural communities. I recognise that research in larger primary schools in urban areas might generate slightly different data. In particular larger schools might well contain more locations in which students could access the Internet. This in turn might create a need for more staff supervision during break times to ensure that on-line students are not "at risk".

With regards to the other fieldwork sites I would argue that the range of broadly typical institutions used in the research ensured that the information gathered could be perceived as being representative of views about the Internet in other post-primary schools. Canalside was a medium sized school in a rural community, while both Dalehouse and Greenswold were large schools in towns surrounded by farming and ex-mining communities. Forestfields was a medium sized school situated in a town that formed part of an urban metropolis. Both Eastway and Hightree were large educational institutions situated close to city centres. In addition to selecting institutions in urban, suburban and rural settings, I also chose schools in affluent and poorer areas. Thus, staff labelled Eastway and Forestfields students as being from affluent backgrounds, whereas they noted that Canalside, Dalehouse and Greenswold schools tended to teach students whose parents were predominantly in the lower income groups. While I recognise that such observations are not scientific measures of socio-economic background, I would nevertheless argue that they provide an indication of class differences.

While the institutions involved in this research contained students with a mix of gender and socio-economic backgrounds none of the schools involved in this research were ethnically diverse. Additionally I did not include any single sex schools in my study. The failure to include ethnically diverse and single sex schools in my research reflected the difficulty of accessing such schools given my research base and obviously limits the generalisability of my results to some extent. Additionally due to practical limitations of time and money all the case studies were located in the north east of England. This means that caution should be used in generalising the findings to other parts of the country, particularly those more affluent areas such as the south east of England.

3. Research methods used

Having considered the research focus, the sampling procedure and the selected fieldsites it now becomes necessary to look at the research methods. A range of data gathering techniques were used including observation, interviews and the content analysis of government publications, school policy documentation and media reports.

Using more than one research method had the advantage that it allowed for triangulation. Denzin (1988) suggests that triangulation might be done in social research by using multiple and different sources (e.g. informants), methods, investigators or theories. During the research, I sought to check the validity of the data gathered through triangulation of sources and methods. In particular I was aware that when talking about Internet use students might downplay aspects of their misbehaviour or exaggerate accounts so that they appeared more skilled or daring. In the first instance, I was able to check that accounts were valid through triangulation across data sources. Hence, I asked other students and staff about particular incidents and compared their responses. The absence of contradiction across a range of different informants suggested that both staff and students were not exaggerating or down playing aspects of school Internet use. Secondly, I used different research methods to triangulate the data gathered. Thus I observed student Internet use to check that their actions did not contradict what they had said during interviews. Furthermore, I was able to ask questions in interviews that allowed me to check whether I had misinterpreted actions, situations or incidents.

Throughout the research process, I sought to ensure that there was internal validity. Referring to the experimental tradition Hammersley notes that "broadly speaking internal validity refers to the issue of whether... manipulation of the treatment produced variation in the outcome" (1992: 66). In the context of case studies, internal validity refers to whether the data gathered has been compromised by changes outside the research process. During my research there was no evidence gathered which suggested that the data was adversely affected by changes outside of my immediate focus. Furthermore, the way in which I carried out interviews and observation remained the same throughout the research, both in and between schools. Additionally I avoided discussing my research data with respondents for fear that I might effect their responses and

invalidate subsequent information. Finally, as will be discussed below, I selected a variety of students, staff, genders, ages, places and times to avoid sampling bias and to foster representation. While I ensured that I interviewed staff of different ages and genders, this did not produce any distinctive patterns when the data was analysed. As my arguments are grounded in the research data I do not therefore consider the issue of school Internet use and gender or staff age in any detail.

Having discussed issues of triangulation and internal validity, I will now consider the research methods used in this research.

3.1 Observation

Since a central concern of the research was students' use of the Internet I felt that observation was essential. In total over one hundred and eighty hours was spent observing student Internet use. For an overview of the total hours of observation spent in each fieldsite school please consult table 2 over the page. Less time was spent in the primary schools with a total of fourteen and sixteen hours observation in Avenue and Brooklands respectively. With regard to the secondary schools, I observed student Internet use for twenty-four hours at Canalside, twenty-six hours at Dalehouse, twenty hours at Eastway, thirty hours at Forestfields and twenty hours at Greenswold. Thirty-two hours were spent observing students using the Internet at Hightree. These observations were spread throughout the period of the research with at least eight visits being made to each fieldsite.

Initially I carried out descriptive observation, noting the details of the setting, the people and the events that took place. Drawing on the dimensions of descriptive data distinguished by Spradley (1980), I collected information relating to space (layout of the physical setting), actors, activities, objects, acts (specific individual actions), events (particular occasions), time (including the sequence of events), goals (what actors were attempting to accomplish) and feelings (evident emotions in particular contexts). I made a record of observations on the spot using condensed language and abbreviations. Shortly after each period of observation I went through these records to add detail and substance as well as to ensure

lucidity and descriptive accuracy. I then typed up full records including running descriptions of events and conversations and adding recalls of any material that I had previously forgotten or omitted from the records (Lofland and Lofland, 1995). Additionally I added any interpretative ideas that I felt might offer an analysis of the situations, personal impressions or feelings, and where appropriate reminders to look for additional information. Having developed a detailed portrait using this descriptive approach I then, drew on this data along with that collected through interviews to develop a set of categories, which were grounded in the detail of the research data (Robson, 1993). I discuss how I analysed and categorised this data later in the chapter.

While the majority of observation was concentrated around the main hub of Internet activity in each school, usually the Learning Research Centre or the main ICT suite, time was also spent observing behaviour in the more peripheral areas of Internet use, such as the subject areas or sixth form bases. As Foster (1996) notes observation can take a variety of forms, differing in terms of the relation of the researcher to participants, the centrality or marginality of the researcher's role, and the degree of overtness or covertness. The vast majority of observation undertaken was non-participatory. A position was taken up, normally at a free desk in the room, the behaviour of students was observed and fieldnotes made. While the actual positions from which the students were observed were never concealed, I found no evidence to suggest that my observation affected students on-line behaviour. Some students accessed websites on "poo", scantily clad women and banned on-line chat rooms despite being observed. Furthermore, while it might be argued that students who were aware that they were being observed might exaggerate their behaviour, accessing unsuitable on-line material in a display of bravado, I found no evidence to support this possibility.

I felt that two factors were important in determining student response to my observation, namely the students' identification of me as someone who was not a member of school staff and my non-interference in their "surfing" activities. For example at Forestfields, three year eight boys accessed what could be labelled as unsuitable websites, kept a watch for members of staff passing through the Learning Resource Centre, concealed what they were doing when staff were

Table 2

Total hours of observation spent in fieldsite schools

Name of School	**Hours of observation***
Avenue	14
Brooklands	16
Canalside	24
Dalehouse	26
Eastway	20
Forestfields	30
Greenswold	20
Hightree	32
Total hours of observation	182

* Observations were spread throughout the research period with at least eight visits being made to each fieldsite.

spotted, and returned to their "surfing" once the coast was clear. In this case in spite of me being the only other person in the room, clearly visible and sitting less than ten feet away the students appeared to pay me little attention. I consider the ethical implications of this incident below. At Brooklands a female student "surfing" on the Internet, looked across the room to see what the teacher was doing before clicking on a web banner that read "Win a million pounds", she did not appear overly concerned by my presence on the next computer along. These illustrations are not especially chosen but are rather typical examples that illustrate the apparent lack of effect of my observation on students.

Adopting a less peripheral role and approaching students who had been the subject of observation tended to result in them initially becoming less animated, often concealing their Internet activities by closing on-screen windows and in some cases becoming clearly uncomfortable. Sometimes it was difficult to get beyond this initial response, yet once the relative inconsequentiality of my role in the school had been re-established, a more participatory style of observation resulted, with students explaining what they where doing and in numerous cases providing practical illustrations of how they were able to hide their activities from teachers. When students were approached, the explanation that the purpose of observation was for research being funded by a local University seemed to sate any curiosity. Indeed no students actually asked questions about the research, merely seeming to accept what they were told at face value. Yet, upon three occasions the students either failed to understand or accept this initial explanation, instead asking which newspaper employed me as a reporter.

Worryingly this more participatory form of observation resulted at Canalside in a student, eager to illustrate the effectiveness of the filtering software, typing the word "porn" into the search engine. Fortunately, the filtering system was effective. Where the observations took place within formal lessons, the teachers introduced me to the group before I circulated around the classrooms, watching student behaviour and asking occasional questions.

Student attitudes to my presence seemed to be summed up by Bill, a year 13 pupil at Hightree, who remarked that "well we keep an eye out for staff. I guess

you're not staff and it's not like you're bothering us, telling us what to do" (Bill, year 13, Hightree). It should be noted that I was dressed not unlike a teacher in a shirt, tie and smart trousers.

Ultimately the actual focus of my observation was twofold, the computer screen and general student behaviour. There were occasional difficulties in seeing what was on a computer screen. While sometimes this problem arose because of the positioning of computers, other times it was because of deliberate attempts by students to conceal their activities from passing staff. This issue is considered in more detail in chapter five.

3.2 Interviews

In all schools I was given permission by senior management to approach both staff and students to ask them if they would consent to be interviewed about their experiences of the school Internet. Both staff and students were free to decline to take part in an interview. However, during the research no one declined to be interviewed. All interviews were recorded using a hand held tape recorder and the dialogues were later transcribed.

Thirty staff in total were interviewed. For details of the staff interviewed please see table 3 over the page. Overall two staff at Avenue and Brooklands, three at Dalehouse and Forestfields, four at Eastway and Hightree, and six at Canalside and Greenswold were interviewed. The person with primary responsibility for ICT in school served as an initial contact, but attempts were also made to interview teachers who had no particular role to play with regard to Internet use.

The member of staff in each school with responsibility for ICT was interviewed at least twice over the course of the research, whereas only eight of the non-Internet related teachers took part in follow up interviews. This mainly reflected the difficulty of locating and arranging to meet staff who had been opportunistically interviewed in the first place.

Interviews with staff tended to last between thirty and fifty minutes. Initial staff

Table 3

Details of staff interviewed

Name of school	Name of staff	Role in school	Sex	Total staff interviewed
Avenue	Ella	ICT co-ordinator	Female	2
	Rick	Head	Male	
Brooklands	Cliff	Head	Male	2
	Jo	ICT co-ordinator	Female	
Canalside	Adele	Science teacher	Female	6
	Maggy	English teacher	Female	
	Ralph	Design teacher	Male	
	Simon	Geography teacher	Male	
	Trevor	Music teacher	Male	
	Wilf	Head of IT	Male	
Dalehouse	Dave	ICT manager	Male	3
	Jenny	Librarian	Female	
	Zed	ICT co-ordinator	Male	
Eastway	Charlie	History teacher	Male	4
	Kent	Art teacher	Male	
	Mary	Head of IT	Female	
	Ray	ICT technician	Male	
Forestfields	Frank	Business teacher	Male	3
	Kate	ICT co-ordinator	Female	
	Liz	Librarian	Female	
Greenswold	Barry	Head of science	Male	6
	Beth	Business teacher	Female	
	Colin	History	Male	
	Hannah	Geography teacher	Female	
	Karen	Geog. / PE teacher	Female	
	Robert	ICT manager	Male	
Hightree	Alan	English teacher	Male	4
	Helena	Librarian	Female	
	Jim	Head of science	Male	
	Tony	ICT manager	Male	
Total number Of staff interviewed			Males 18 Females 12	30

interviews were formally arranged, but as the research progressed more use was made of opportunistic interviews. Only at Greenswold, thanks to the efforts of the ICT manager, was it possible to formally arrange a series of interviews with five randomly selected teachers. Otherwise contact with staff without formal responsibility for the Internet tended to be opportunistic. Indeed over half of the staff interviews conducted in the post-primary schools were opportunistic, with contacts frequently being made in staff rooms. Although staff who used the ICT areas were also approached to take part in the research, it was felt that using the staff room as a point of contact enabled the inclusion of those who might be less inclined or less able to use the Internet. In such situations I made it clear to staff that their views mattered regardless of the extent of their on-line expertise.

In total sixty-three students were interviewed, thirty-two male and thirty-one female. For details of the students interviewed please consult table 4 over the page. The interviews at Avenue (four students) and Brooklands (four students) tended to be informal involving students who were actually "surfing" the web at the time, asking them about their current activities, how this related to general internet use and what problems, if any, arose from using the Internet. Additionally eight students were interviewed at Canalside, Greenswold and Eastway, nine at Dalehouse and Forestfields, and thirteen at Hightree. Interviews with students tended to last fifteen to twenty five minutes. The vast majority of student interviews in the post-primary schools were opportunistic with on-line students pausing in their "surfing" activities until the interview was complete. In situations where a pair or group of students sat a terminal "working" together attempts were made to include everyone in the discussion.

While some of the students seemed nervous about being interviewed none of them actually refused. However, four interviews were abandoned where the interviewee proved uncommunicative and unwilling to engage in conversation. This happened once at both Forestfields and Greenswold, and twice at Dalehouse. On all four occasions, with no other explanations forthcoming, I felt that despite giving permission for the interviews the four boys felt intimidated by the situation. The information from these interviews produced no useful insights

Table 4

Number of students interviewed by sex and school year

Name of School	Students interviewed by sex and school year	Total number of students interviewed
Avenue	2 males year 6 1 female year 6 1 female year 4	4
Brooklands	1 male year 5 2 females year 6 1 female year 5	4
Canalside	2 males year 10 3 males year 8 2 females year 10 1 female year 7	8
Dalehouse	3 males year 10 1 male year 9 1 male year 7 2 females year 11 2 females 7	9
Eastway	1 male year 13 3 males year 10 1 male year 8 2 females year 12 1 female year 10	8
Forestfields	1 male year 13 2 males year 9 1 male year 7 1 female year 12 2 females year 11 2 females year 8	9
Greenswold	1 male year 12 1 male year 11 1 male year 10 1 female year 13 1 female year 12 2 females year 9 1 female year 7	8
Hightree	3 males year 13 4 males year 12 2 females year 13 4 females year 12	13
Total number of students interviewed	Male 32 Female 31	63

and was excluded from the final count of students successfully interviewed. Where possible an attempt was made to interview students a second time after almost a year had passed. This was possible with one student at both Eastway and Greenswold, two at both Dalehouse and Forestfields and three at Hightree. Attempts were also made in all schools to interview students found outside of IT suites, who declared a lack of Internet knowledge and experience. This was done to try to avoid a possible bias that equated student views about the Internet solely with those who made use of it. In total twelve students who claimed to avoid using the school Internet were interviewed across all post-primary schools. Although due to the small number I felt that any views could not be considered representative, it was a useful exercise in attempting to avoid bias in sampling. Beyond these twelve students generally having little to say about the Internet these interviews revealed no additional information.

Initial interviews tended to concentrate upon general Internet use in schools. As the research developed and the focus was refined a list of more specific questions was drawn up. These questions more directly addressed issues of the nature of on-line risks and attempts at controlling Internet use. The intent was not for this list of questions to be used rigidly but rather to provide a way to begin to address some of the issues relating to risks arising from school Internet use. Respondents were encouraged to discuss at length some of the issues raised. Indeed where possible they were allowed to address the concerns that they felt were important. I felt that as the research was an exploratory investigation it was vital that respondents be allowed some influence over the issues covered.

Upon two separate occasions incidents occurred relating to the recording of interviews. When Mary, the IT Head at Eastway, was asked what she thought of the ideas put forward by an LEA ICT consultant, she replied that while happy to discuss the subject the tape recorder should be turned off while she did so. This was duly done, she expressed her opinions, the tape recorder was switched back on and the interview continued. The second incident which occurred towards the end of the research was perhaps more problematic. Two teachers at Canalside agreed to be interviewed but refused to allow the discussions to be tape-recorded. Although this made the interviews more difficult insofar as extensive field notes

had to be taken the teachers were willing to discuss a whole range of Internet related issues. The following day the ICT manager at Dalehouse offered an insight into the possible reasons for this refusal to be tape-recorded. After I had related this occurrence to the ICT manager, he described how some parents at Dalehouse had recently brought tape recorders into meetings with teachers. Understandably the teachers were concerned at this turn of events, worried that their spoken words would be recorded and possibly used against them. Such actions leading to the reluctance of teachers to take part in recorded interviews could have serious repercussions for future educational research.

Broadly, the research could be labelled as overt, insofar as schools, staff and students were openly informed that the focus was Internet use. However, as the research progressed and the issue of risk and Internet misuse became more prominent it was felt that it would be counterproductive to highlight this particular aspect. Internet misuse was an area that a few ICT staff appeared reluctant to dwell on in interviews. Indeed the Head of IT at Canalside implied that such a concern was negative and unhelpful. Arguably, such a view mistakenly confuses the academic examination of a negative issue with its sensationalistic reporting in the media.

3.3 Content analysis

Three main sources of documentation were used in the research; namely, government literature, media reports and school based information. A wealth of documentation has been generated around "the Learning Grid". From policy statements (DfEE, 1997a), to reports on effective use (BECTa, 1998) and information packs that seek to ensure safe on-line "surfing" (DfEE, 1999). This material occupies a central position in the discursive construction of Internet use. Recognising this a range of academic writing deconstructing this literature has swiftly emerged (Selwyn, 1999a; Selwyn, 1999b; Moran-Ellis & Cooper, 2000). Furthermore media reports on television, radio, the Internet itself and in newspapers, detailing a whole range of Internet related stories are rife. Occasionally sensationalistic such reports serve to construct the popular conception of the benefits and dangers of the Internet. Beyond such

considerations the media also provided accounts of incidents which I used when attempting to assess whether certain risks were actual or perceived. Finally schools themselves produced a range of information, from reports relating the number of students and Internet machines, to policies attempting to construct and encourage effective Internet use. As discussed in chapter nine Acceptable Use Policies (AUPs) and posters providing guidelines were central to schools' Internet rhetoric. I analysed such material by focusing upon the symbols and words used and seeking to expose both the inherent and underlying messages. Additionally I sought to determine the values embodied in the particular content. Once I had analysed the various materials I wrote up notes and integrated these with the rest of my research data. An analysis of these sources provided a rich foundation on which to build an informed discussion of the schools' attempt to introduce ideas of appropriate Internet use.

4. Analysis of research data

As Robson notes "the fact that a study is a case study does not, in itself, call for a particular approach to the analysis of the qualitative data which it produces" (1993: 473). While my analysis of data gathered from the case studies drew upon elements of grounded theory (Glaser & Strauss, 1967: Strauss & Corbin, 1990), it was also informed by writings on sophisticated "subtle" realism in ethnography (Hammersley, 1992).

According to Hammersley (1992, 50-54) subtle realism is concerned with defining knowledge as beliefs about whose validity we are reasonably confident. Furthermore, this approach acknowledges that there are phenomena independent of our claims about them, which those claims may represent more or less accurately. Finally, the overall research aim of subtle realist approaches is to represent reality while acknowledging that such a representation will always be from a particular perspective that makes some features of the phenomenon relevant and others less so. Such considerations were useful when thinking both about the research methods and data collected, as they encouraged a more reflexive approach.

As Robson (1993) notes, it is usual for case studies to be neither exclusively ethnographic nor grounded theory studies. I sought to draw relevant elements from both approaches. Hence, I generated relevant categories from the data gathered using certain grounded theory techniques (discussed below), at the same time seeking to understand the perspectives of others and limitations of the research process. While writings on grounded theory influenced my coding and analysis of data, knowledge of subtle "realist" approaches ensured a more reflexive approach when considering the research data and hermeneutically interpreting others views.

In summary this research should be seen neither as a straightforward example of grounded theory nor of "subtle" realist ethnography, rather as a combination of selected elements of both.

While I had a pre-existing knowledge of the sociology of risk literature it did not in itself provide me with an analytical framework. Rather writings on risk offered inspiration while I was analysing the research data. For example, I came across Oswell's (1998) article on children and Internet content regulation while sorting out the initial confusion created by staff discussion of risk processes and outcomes. Having already separated the data on staff risk perceptions into categories concerned with students "in danger" and as "sources of danger", Oswell's article helped to clarify my thought process, enabling me to label these two categories "students-at-risk" and "dangerous students".

During the research process I went through an almost constant process of reading and re-reading the data collected from interviews, observation and content analysis. All this information was kept in the form of typed transcripts on computer disks. Each period of observation or interview was referenced according to time, date, individuals involved, and institution. I got to know the data well and wrote down any thoughts that arose in the forms of memos. I realised that I needed to start developing categories early in the research process to impose some kind of order on the data.

Drawing on certain techniques from grounded theory, I sought to explain what was central in the data. Thus, the categories I initially developed came from the data. Searching for themes I split the data (interview transcripts, field notes, document analysis) into discrete parts of a sentence, utterance or paragraph. I then considered what the data was an illustration of and attached an appropriate code. The code in this sense can be seen as a label and initially such codes were provisional. As I felt that some data fell within more than one conceptual category in some instances, I applied several labels to the same piece of data. Initially the labels I applied were quite broad. For example a segment from an interview with a member of school staff where the dangers of on-line pornography were mentioned would have been initially labelled as staff (role, institution including age range) interview, risk, pornography. While such broad open coding was initially useful in sorting through the masses of data it tended to lack any sophistication. I set up computer files and copied the discrete labelled data into relevant categories. Emerging from the data initial categories were labelled amongst other things by specific risk processes (e.g. on-line pornography, chat-lines, racism), control procedures, interpretative difficulties and viewpoints on staff / student roles. At this stage I was aiming to tease out the theoretical patterns in the data. Where data was relevant to several key emerging categories I copied the information into all the files that I felt were relevant.

I constantly questioned whether the categories and sub-categories I was creating were embedded in the data. Indeed when considering the nature of on-line risks I had initially come up with a long list of possible dangers, including on-line bullying, Internet addiction, repetitive stress injury. However, I realised that these particular categories did not come from the data and I decided that I would concentrate on the dangers that emerged from my case studies. Having given codes to the data, I examined new information looking for similar phrases and themes.

As the research progressed, there was a shift from an initial concern with describing events and processes to interpretation (Wolcott, 1994) and I refined my somewhat crude categories, making qualitative judgements about observations and quotes. For example, when starting to analyse staff perceptions

of Internet risk I became aware that simple references to on-line pornography or chat-lines were not in themselves sufficient to argue that staff were concerned about these possible dangers. Rather I interpreted and analysed what was actually said, asking whether there was firm evidence in the data that staff were worried about particular on-line dangers. For example, one member of staff described an American university fraternity website that condoned drinking excessive amounts of alcohol. However, she discussed this website, which she had found while looking for information on alcohol abuse for a humanities course, in a manner that indicated she did not see it as dangerous. Hence, I did not include her comments when analysing staff concerns about websites that encouraged experimentation with drugs.

When refining different categories of on-line risk within the data it became evident that interviewees initially had a tendency to focus on risk processes. For example, staff would talk about the dangers of pornography without initially been explicit about what they felt the outcome of these dangers might be. I became aware of this factor in the initial interviews and was therefore able to ensure that I always asked follow up questions about the perceived risk outcomes. Data was subsequently collected which suggested that while individuals might talk about, for example, the risk of on-line pornography in some instances the student was seen as being at risk while in others they were descried as posing a danger to the school through their on-line activities. This suggested the existence of new categories relating to who was perceived to be at risk. At this time, I came across Oswell's article on children and Internet content regulation. Although this work was an analysis of government policy discourse, it proved very useful in suggesting labels, which I could apply to these newly emerging categories. While I used Oswell's article to assist my thought process, particularly with reference to the actual naming of the categories, it should be noted that the categories of the "student-at-risk" and "dangerous student" emerged initially from the data.

While carrying out open coding, I noted any idea that occurred from working with the data about relationships between the categories and initial thoughts on what the core categories might be. This analytical process was ongoing while

data were still being collected. Towards the end of the research process itself many of the categories became "saturated" insofar as continued analysis was producing severely diminished returns in terms of new categories or insights.

Having split the data through open coding I then started through axial coding to consider the relationships between the categories. Axial coding involves assembling the data in new ways after open coding in an attempt to identify central phenomenon and explore conditions as well as consequences (Robson, 1993: 194). Thus I sought to draw out an understanding the central phenomenon of school Internet risks. I considered the context of risks and risk perceptions, the action and interaction strategies arising from school Internet risk and the consequences. Through this analytical process I was able to establish that risk perceptions were connected with student age and the institution attended. Thus with reference to school Internet use primary school students were labelled by staff as being "at-risk", whereas in secondary and post-16 institutions the student was often described as being a source of danger. This issue is discussed in more detail in chapter four. Having explored conditions and relations in the data I then progressed to selective coding.

Selective coding seeks to integrate the categories in the axial coding model (Robson, 1993: 194). In this stage conditional propositions are typically created. While the grounded theory approach seeks through selective coding to select one aspect of a core category and focus on it I felt that it was important that I concentrate equally on risk perceptions, risk assessment and attempts to alleviate dangers. Although it might be argued that the category of school Internet risks provides a central integrating focus I have chosen not to focus at this level of abstraction. Rather in chapter twelve I have sought to make claims both about the risks relating to school Internet use and contributions that this research makes to the sociology of risk. I also argue in the final chapter that to comprehensively understand risk from a sociological perspective researchers should consider risks perceptions, assessment and control. These arguments which emerged from my data, resulted in a limited rather than absolute application of selective coding.

5. Ethical issues

Two main ethical issues emerged during the research relating to the asking of questions about on-line pornographic material and the observation of students misusing the Internet. I will deal with each of these ethical issues in turn.

In interviews the question of the risks posed by Internet use occasionally led to a discussion of pornography and on-line sexual conversations. Staff were free to discuss the issues that they felt relevant to Internet use. However, I was aware that if they mentioned sexual material I needed to ask supplementary questions relating to the actual type of material, the dangers posed by such items and the potential victim of these risks. Clearly this was an embarrassing issue for some staff that they would have preferred to gloss over. Yet if the research was to be a valid representation of Internet risk perceptions I needed to ask such questions. Hence, while I never directly brought up the subject of on-line sexual content, when the topic was broached I subsequently asked a range of supplementary questions. While this may have caused discomfort for some teachers only on one occasion did a respondent ask me to change the topic. On this occasion Cliff, the Head of Brooklands, after having answered a question about on-line pornography and home Internet access stated that:

> I think this is not really a potentially helpful line of questioning. I've said all I wish to say on that particular subject. Either we discuss something else or the interview is at an end (Cliff, Head, Brooklands).

Discussing the issue of on-line sexual content with students was potentially more problematical. After all, I was keen to avoid causing them discomfort or encouraging them to misuse the Internet. I avoided the issue of on-line pornography unless raised by the student. Depending on the age and response of the student I then made a decision whether I should ask supplementary questions. It should be noted that the questions I asked the students about on-line sexual material were less direct and couched in more general terms than those posed to the staff. I was careful to avoid causing discomfort to students by asking embarrassing questions that made them uncomfortable. Indeed when I interviewed children in primary schools I encouraged them to "surf" on the

Internet while I asked them about the websites they visited and occasionally questioned them about problems, difficulties or things that were "not good" on-line. While this sensitive approach to interviewing children about potentially embarrassing subjects reflected a genuine concern for the welfare of the students I was also aware that if schools perceived me as focusing directly on such topics they might withdraw permission to interview students.

The second main ethical issue related to my observation of students misusing the Internet. None of the schools in which I carried out research asked me to report students seen abusing the school Internet. I concluded that as long as I judged the students to not be in danger from their on-line activity or breaking the law my role would remain that of the observer. There were some minor incidents where I questioned this role but nothing I saw motivated me to act. For example, a group of three year 8 boys at Forestfields using the Internet after school accessed a website called *Poo III*, which had a digitised photograph of a person eating excrement. Yet, this picture seemed to be merely a source of great amusement to the students who appeared more interested in reading the websites poems about defecation. Importantly throughout the research no individual was seen accessing illegal material on the web.

In conclusion I would argue that because of the nature of Internet risks some ethical issues such as the subject matter of interviews and observing "net" misuse inevitably arose. Yet I would maintain that such issues were resolved with a sensitive, reflexive approach that took account of the concerns of students and staff.

Conclusion

In this chapter, I have outlined the research focus, sampling techniques, research methods, process of data analysis and ethical issues. In so doing I have added detail to the research background. The first three chapters can be seen as providing a framework for this research. Thus, I have considered the rationale for the research (chapter one), the relevant literature (chapter two) and the research process (chapter three). Having provided this background it now becomes

necessary to consider the data gathered. In chapter four I focus on the staff perceptions of Internet risk, in chapter five I consider the student risk narrative and in chapter six I examine the problematic interpretation of on-line material. Overall, the next three chapters describe school Internet risk perceptions, which I subsequently assess in chapters seven and eight.

Part Two

Staff / student perceptions of risks arising from school Internet use

In chapter four I describe the staff perceptions of risks arising from school Internet use. In chapter five I focus upon the student view of risks surrounding the school Internet. Finally in chapter six I consider how concepts such as "pornography", "hateful" or "dangerous", which have been used to describe risks in the previous two chapters, are social constructs that give rise to interpretative difficulties.

Chapter Four

Staff perceptions of risks arising from school Internet use

Introduction

Any attempt to fully understand the risks surrounding school Internet use needs to start with a description of the relevant narratives. In this chapter I describe the staff perceptions of Internet risk. The student risk discourse is the subject of the following chapter. Staff concern about the dangers arising from school Internet use focused upon the issues of on-line pornography, chat-lines and electronic mail, hate engendering sites, experimentation websites encouraging the manufacture of explosives or drugs, copyright and network security.

Overall thirty staff were interviewed, two at Avenue and Brooklands, three at Dalehouse and Forestfields, four at Hightree and Eastway, and six at Canalside and Greenswold respectively (see table 3 for further details). While the person with primary responsibility for the school Internet served as the initial respondent in the schools, attempts were also made to interview teachers who had no particular role to play with regard to Internet use. The staff interviews took place in the schools themselves and tended to last between thirty and fifty minutes. All staff interviews were tape recorded and later transcribed for analysis, with the exception of one session at Canalside. In this particular case staff agreed to be interviewed on the condition that the session was not tape-recorded.

Of the thirty staff who were interviewed twenty-eight expressed concern about pornography, twenty-four about chat-lines, three focused on hate engendering sites, two were worried about experimentation websites, seven considered the legal threat arising from copyright violation and nine discussed the dangers posed to network security. In discussing their concerns, staff drew variously upon the narratives of the "student-at-risk" and the "dangerous student". In conclusion, I note that students engaging in hazardous Internet activities in primary schools were seen solely as being at risk, while in the post-16 institution they were labelled as dangerous. In secondary schools both narratives of the student being

at risk and / or dangerous were used when describing on-line hazards. These themes will be considered in detail as I now analyse the staff risk narratives on pornography, chat-lines, "hate sites", experimentation, security and copyright.

1. Pornography

Twenty-eight of the thirty staff interviewed raised concern about students accessing pornography using the Internet. Two of those interviewed were unable or unwilling to expand upon the issue of who was in danger from pornography or what the hazardous outcomes might be. Of the remaining interviewees eighteen focused upon the threat that students accessing pornography posed to the school, five were solely concerned that students were at risk from unsuitable images and three expressed worry that students were at risk while also being a threat. Two members of staff did not see on-line pornography as a danger. No primary school teacher discussed on-line pornography in terms of students deliberately accessing such material and posing a threat to the school image. Focusing in turn upon the primary schools, the secondary schools and the post-16 college I will now consider staff risk narratives concerning on-line pornography in more detail.

1.1 Primary schools

Three out of four primary school teachers interviewed expressed concern about on-line pornography. These concerns focused not upon students wilfully seeking unsuitable material, but rather on the possibility of students accidentally stumbling across such items while "surfing". Rick, the Head of Avenue primary school remarked that:

> Well I suppose pornography is a concern, especially when you're talking about children, especially young children accidentally coming across it ... Young children tend to be quite impressionable so it's obviously important that we protect them from exposure to such unsuitable material (Rick, Head, Avenue).

Rick perceived the danger of on-line pornography in terms of students unintentionally stumbling across explicit material. Insofar as Rick labelled young

children as impressionable I would argue that he invoked a narrative of innocence, suggesting that young students are easily influenced and need protection. Thus, the students were depicted as being at risk from accidentally accessing material. While not explicitly stating the nature of the risk outcome, Rick remarked that young children are impressionable implying that his concern lay with the psychological development of the child. Ella, the ICT co-ordinator at Avenue primary school shared this concern about the need to protect students from accidentally stumbling across pornographic material on-line. She noted that while such material was blocked by the filter system, she checked websites the students might access to see if there were any "bad sites". This action arguably revealed a concern about the effectiveness of the Internet filtering system. Indeed despite the apparent effectiveness of filtering software Ella noted that search engines sometimes listed websites with unsuitable and even obscene titles. She commented that regardless of students' ability to access pornographic websites "you do get the names of sites that could be interpreted badly" (Ella, ICT co-ordinator, Avenue). In conclusion, Ella was not concerned with students deliberately accessing unsuitable pornographic material, remarking that "we haven't actually had a problem with anybody accessing anything that they shouldn't have been" (Ella, ICT co-ordinator, Avenue).

Cliff, the Head of Brooklands primary school, couched his concern about on-line pornography in terms of students unintentionally accessing material. Indeed for Cliff the inevitability that students might stumble across unsuitable on-line material raised an important question of whether, knowing this, parents would still be willing for their child to use the Internet.

> Pornography is there all the time. It is always a click away from somebody's child, for whom you have the care, whose parents may not want their children to even have a quick glimpse of something of that nature. Parents have to realise that children are going to be using the Internet at school. There's a chance that they [the student] see this sort of material. Do they accept the risk or do they say I don't want my child to use the Internet (Cliff, Head, Brooklands).

Cliff expanded upon this idea that on-line pornography might only be a click away in his explanation of why students did not have Internet access in the

reception class. Here the issue was not just the likelihood of unsuitable material being assessable but also the undiscerning way in which younger students used the Internet. Thus Cliff noted that the reception class in year one were not allowed to access the Internet because of the non-selective way in which they used computers, randomly clicking on hyper-links.

Indeed drawing on Cliff's observation it can be argued that if students using the "net" are to be labelled as "dangerous" they need an awareness of the existence of unsuitable material, a desire to find it and an ability to effectively "surf" the web. To the extent that young children lack these drives and abilities I would argue that they should not be seen primarily as posing an on-line danger to the school. Interestingly Jo, The ICT co-ordinator at Brooklands Primary School, did not see on-line pornography as a risk. She justified this assessment remarking that "[t]he filtering [software] is effective. The children are not going to blunder across unsuitable images, at least not using the school Internet" (Jo, ICT co-ordinator, Brooklands). In using the term "blunder" I would argue that while Jo did not see on-line pornography as a risk she nevertheless privileged the narrative of students accidentally rather than deliberately accessing such material.

Staff concern about the Internet and pornography in primary schools was versed in terms of the risk that students might accidentally access such material. This anxiety arose partly from the belief that young children might not be discerning "surfers", instead randomly pointing and clicking at icons. It could also be argued that younger children are not necessarily interested in pornographic material. Thus, I would maintain that sites featuring cartoons, such as the *Simpsons*, or pop stars, such as Britney Spears, hold more appeal for younger children than pornographic websites. Indeed in an incident at Brooklands a student who managed to steal his older sister's password and gain access to the school Internet, was found attempting to access the *Simpsons* cartoon site rather than "adult" websites. While discussion of risk outcomes tended to be minimal, conversations about impressionable children indicated that teachers' concern was focused on the issue of psychological development. Thus, Rick talked about the children as "impressionable", while Ella was worried about website names that might be interpreted negatively. Having examined the narratives concerning the

risks posed by on-line pornography in primary schools, I shall now consider the issues raised by staff in secondary schools.

1.2 Secondary schools

Whereas in the primary schools students were seen solely as being at risk from accidentally accessing pornographic material, in secondary schools staff concerns about "dangerous students" deliberately "surfing" for unsuitable material were prominent. This is not to suggest that staff were unconcerned with the potentially detrimental psychological effects of on-line pornography, but rather to highlight that anxieties about the school image or student control emerged.

At Canalside secondary school Wilf, the Head of IT, expressed concern about Internet pornography while pointing out that such material existed in wider society. Thus he argued that:

> Well the obvious dangers that come to my mind are to do with pornography, that sort of abuse ... It's just a reflection of normal life. If they [students] can't get material on the Internet they will just get it from somewhere else" (Wilf, IT Head, Canalside).

Two points can be made about Wilf's remark. Firstly, he saw on-line pornography as abuse. While this statement might be interpreted as a wider social critique of an exploitative industry, he subsequently discussed at length the issue of students misusing the Internet. In this context, the abuse can be interpreted in terms of students misusing an expensive piece of school equipment. Secondly, he sidelines the issue of psychological harm from unsuitable on-line material, arguing that if students want to access such images they will get them from somewhere. These two points seem to indicate that Wilf is not so much concerned with possible harm to the students but rather inappropriate use of the school Internet system. Ralph, a design and technology teacher at Canalside noted that "porn can be a problem, you need eyes for twenty one kids it's just impossible to see all the screens at once" (Ralph, design and technology teacher, Canalside). Having expressed concern over pornography and control issues in class, Ralph subsequently advised me, while laughing, to interview a particular

student, Phil, who had been banned from using the school Internet after having accessed pornographic material. Simon a geography teacher at Canalside initially remarked that accidentally coming across pornography was unlikely due to the effectiveness of the school filtering software. He later noted that students deliberately seeking to access pornography was an issue, particularly as they were proving increasingly good at avoiding accountability for their actions through swapping and stealing passwords. Trevor a music teacher and Maggy, an English teacher, both expressed concern about on-line pornography remarking upon the difficulty of constantly keeping an eye upon what they respectively referred to as "trouble-makers" and "unruly students". In this context, I would argue that the students were primarily perceived as dangerous insofar as these teachers labelled them as disruptive and in need of constant surveillance. Adele, a science teacher argued that on-line pornography was a risk but subsequently failed to expand upon this assertion. Indeed, when I asked her who was at risk from pornography she deliberately changed the subject to the numerous educational benefits that she believed the school Internet offered. A failed attempt to return to this issue later in the interview might be taken as an indication that accessing pornography on the school Internet was not a subject which Adele wished to discuss. Nevertheless, overall the narratives engaged in by staff at Canalside tended to label the students as dangerous, insofar as they were perceived as deliberately "abusing" the Internet, causing "trouble" and needed to be keenly watched.

At Dalehouse secondary school concern about students accessing pornography focused upon the possible detrimental effects to the school and the student. In discussing students accessing pornography Dave, the ICT manager and part-time geography teacher, remarked that "it's a problem if they access porn. But more as a discipline issue" (Dave, ICT manager, Dalehouse). Indeed when discussing a student who had set up his own pornographic website at home so that his friends could access it from school, Dave remarked that "it makes you think he's got good IT skills. Still that sort of thing can reflect badly on us. We had the site cut out and told his parents what he was doing" (Dave, ICT manager, Dalehouse). While Dave saw students accessing pornography as potentially reflecting badly upon the school, Zed, the ICT co-ordinator and Jenny the librarian were

concerned with the effect that the material might have on the students. Zed noted "although we've got a pretty good filter, it is a worry that there's some pretty sick stuff on-line" (Zed, ICT co-ordinator, Dalehouse). Additionally Jenny expressed concern for the younger students remarking that "well with the younger ones who haven't already been exposed to sex and things it could affect them" (Jenny, librarian, Dalehouse). Unspoken here was not only the way in which pornography might affect students but also the assumption that older students were less at risk insofar as they had probably already been exposed to such material.

At Eastway secondary school, Charlie a history teacher, recognised that the risks arising from accessing pornography on the school Internet might vary depending upon the perspective adopted. While drawing attention to the issue of age, he noted that the risk outcomes might relate to psychological effects, staff authority and school image.

> Well I guess the porn could be a problem. Particularly with the younger ones, you don't want them seeing stuff that could disturb them. But even with the older ones ... I wouldn't want students accessing that sort of material while under my supervision. In some ways, it's a challenge to my authority.... And that's not to mention the school image (Charlie, history teacher, Eastway).

Thus Charlie recognised that the risks of on-line pornography might not just threaten the student but also the teacher and school. Yet none of these risk outcomes are mutually exclusive. After all, a child deliberately accessing Internet pornography in a lesson might be psychologically affected, while undermining the authority of the supervising teacher and threatening the image of the school. When the Internet was first installed in school Mary, the Head of IT at Eastway, expressed concern about students accidentally accessing unsuitable material. After six months, during which time Mary argued that the filtering software had proved effective, she became more concerned with students deliberately accessing porn. While Mary noted there were few incidents, she indicated that such transgressions were an affront to her and the school. Ray, an ICT technician, shared Mary's view arguing that "some students think they can get away with it. I'm sure they see it as some kind of game. Thinking, they [the students] can put

one over on us [the staff]" (Ray, ICT Technician, Eastway). In this sense the students were viewed as playing a game in which they challenged staff and school authority. The other member of staff interviewed at Eastway, Kent, did not see on-line pornography as a risk. Rather Kent, an art teacher and union representative, expressed anxiety about chat-lines, the increased use at home of personal resources for schoolwork, the demands to attend unpaid Internet training sessions and the personal risk of copyright violation as problematic issues.

At Forestfields secondary school the concern seemed to focus on both the accidental and deliberate accessing of on-line pornography. While Kate, the ICT co-ordinator, in response to a question concerning on-line risks, related two incidents where students had deliberately accessed material of a sexual nature, she also later told how a student searching for information about Crystal Palace had stumbled upon a website dedicated to a porn star of that name. The librarian, Liz, who observed students using the Internet in the LRC, explained that "I'm concerned not just with students actually seeking certain images, though I can control that by watching them, it's also students just coming upon certain images" (Liz, librarian, Forestfields). Discussing on-line risks, Frank, a part-time business studies teacher at Forestfields remarked that "I guess porn is a problem for a lot of schools" (Frank, business studies teacher, Forestfields). However when I asked why and to whom it was a problem, he was unable or unwilling to answer.

At Greenswold secondary school the issue of students accessing pornography was clearly related to concern about staff authority and school image. Indeed Robert, the ICT manager at Greenswold compared students accessing on-line pornography with bringing "mucky magazines" into school. He argued that such incidents reflected badly upon the school.

> The porn worries me to be honest only more from the image point of view. The kids I'm talking about are accessing it outside, so any damage that is done to them is already done. But the damage that can be done to our image is enormous (Robert, ICT manager, Greenswold).

Thus Robert asserted that students wilfully accessing pornography on the school Internet had probably already accessed such material outside school. His concern was not with the "student-at-risk", after all the damage was already done. Rather Robert was worried about the "dangerous student", whose activities if publicised threatened the reputation of the school. Karen a geography and physical education (PE) teacher at Greenswold remarked that on-line pornography was a problem, "I mean first lesson I had in the computer room that [pornography] was all they were interested in" (Karen, geography and PE teacher, Greenswold). In a similar vein Colin, a history teacher at Greenswold claimed that "I mean the kids just mess about and they're obsessed with getting the porn" (Colin, history teacher, Greenswold). Both Karen and Colin in expressing concerns about on-line pornography described students as deliberately seeking out such material. Indeed both teachers went on to discuss the difficulties of controlling classes that were using the Internet. This suggests that accessing pornography might be seen as a challenge to teacher authority. Hannah, a geography teacher at Greenswold and Barry, the Head of science at Greenswold, saw the threat posed by on-line pornography in terms of the school image and their own authority. Hence Hannah remarked "it's [pornography] just another potential discipline problem for teachers, for the school" (Hannah, geography teacher, Greenswold) while Barry maintained "it [students accessing pornography] reflects badly on me and it could reflect badly on the school" (Barry, Head of science, Greenswold). While Beth, a business studies teacher at Greenswold, shared this concern about students deliberately accessing pornography she also noted that students might stumble across unsuitable websites which had been given innocent addresses. For example she related that "there's a website that's basically a porn site, that's called bank.account.com" (Beth, business studies teacher, Greenswold). Nevertheless during the interview Beth did not express any concern about the damage that might be done to students. Rather she went on to suggest that if staff unwittingly allowed students to access on-line pornographic material in class then "you leave yourself open to criticism" (Beth, business studies teacher, Greenswold). In this case, Beth suggested that the criticism was more likely to come from peers and school management than students.

Overall concern about accessing on-line pornography in the secondary schools related to both the "dangerous student" and the "student-at-risk". Notably where staff, such as Jenny at Dalehouse, did express concern about the risk to impressionable students it tended to be focused on younger children. In comparison to the two primary schools staff concerns about Internet pornography in the secondary schools were more focused upon students deliberately accessing unsuitable material and the threat this posed to teacher authority and school image. To ascertain whether similar views existed in all the post-primary institutions included in this research I will now consider staff risk narratives about on-line pornography in the post-16 college.

1.3 Post-16 institution

Early in the research the ICT manager at Hightree, Tony, had highlighted concerns about students accessing pornography on the college Internet. For him the staff and the college rather than students were at risk. He argued that accessing pornography was an affront to the supervising teachers and threatened the good name of the institution. Indeed Tony later justified the expulsion of a student for accessing a pornographic website with reference to the fact that it had offended a female teacher who was present. When I asked whether the students themselves were at risk from on-line pornographic material the following discussion ensued:

> Interviewer: But what's the danger to students of accessing such material [porn]?
> Tony: Well the real danger is that they access it at all.
> Interviewer: Why?
> Tony: I don't quite follow ...
> Interviewer: What is the consequence of them accessing such material?
> Tony: If we catch them they'll be punished.
> Interviewer: But beyond that what danger does pornography pose to the student?
> Tony: Well I've already said...
> Interviewer: For example might the risk be psychological?
> Tony: You'll have to explain that.

Having explained my question to Tony, he argued that such considerations were not an issue. Arguably this reflected the view that in a post-16 institution the

students were considered young adults, not impressionable children. According to Tony the issue of students accessing pornography was seen purely in terms of potential negative outcomes for the staff or college. Thus he remarked:

> The students are old enough, they know what's acceptable. If they access unsuitable material they will be punished. After all we need to maintain discipline and protect the good name of the college (Tony, ICT manager, Hightree).

This is not to suggest that students were likely to be punished for accidental "net" misuse but rather that the staff interviewed felt that the students were sufficiently mature to behave responsibly if they stumbled across unsuitable material. Both, Jim the Head of science and Helena, the college librarian, supported this view maintaining that "students are old enough to know what they are doing" (Jim, Head of science, Hightree) and that "they [students] are well aware of the rules, they should know how to behave" (Helena, librarian, Hightree). Alan, an English teacher at Hightree, remarked that "we're not so much bothered about the impact of porn on the students because they're young adults, not children" (Alan, English teacher, Hightree). As Alan went on to note children are more impressionable and vulnerable than adults. Interestingly Alan was the only person interviewed in the research to touch upon the issue of staff using the Internet to access pornographic images. He related how at a school he had worked at previously a music teacher had been arrested for downloading child pornography using his home Internet. It is worth noting that no concern was expressed during the research that illegal pornography might be accessed in school.

1.4 Summary

In conclusion it can be seen that in primary schools staff were concerned with students being at risk from accidentally accessing pornographic images, whilst in the secondary and post-16 institutions anxiety tended to focus more around the student deliberately seeking such material and threatening the school image or staff authority. Indeed in the Further Education college staff expressed no concern for the impact viewing on-line pornography might have on the students.

Referring to the students age's staff noted that they should not deliberately undertake such activity in college. Having considered staff concerns about on-line pornography I shall now focus on anxieties arising from student use of chat-lines in school.

2. Chat-lines and electronic mail

Spread across all eight schools twenty-four of the thirty staff interviewed expressed concern about students using the school Internet to access on-line chat rooms. Only Tony, the ICT manager at Hightree, discussed the possible abusive use of the school e-mail system. While ten staff were exclusively worried that students were at risk from undesirable language and strangers, a further ten tempered this concern with the view that students accessing chat-lines were also abusing resources in a manner that could damage the school image. Four staff discussed student use of chat-lines entirely in terms of the threat posed to school image and resources. Notably the teachers interviewed in primary schools described children in chat rooms as being at risk while three out of four staff at the post-16 institution described the students' on-line "chatting" activities as a threat to the college.

2.1 Primary schools

In the primary schools chat rooms were seen as "risky" insofar as they gave strangers access to impressionable young children. While maintaining that he felt it was a remote possibility, Rick, the Head of Avenue, expressed concern that students might be persuaded to meet up with people who they'd chatted to on-line. Indeed he noted "I suppose it's always a threat that children might be enticed to meet up with someone they've met on a chat-line" (Rick, Head, Avenue). Ella, the ICT co-ordinator, remarked that on-line chat rooms were a worry, commenting that "if chat-lines aren't moderated the language can be quite offensive" (Ella, ICT co-ordinator, Avenue).

Cliff the Head of Brooklands was particularly worried about unknown adults using on-line chat rooms to nurture relationships with young children. He

maintained "chat-lines are so open. It's like citizen band radio on the computer. And you really don't know who you are actually talking to. They can claim to be whatever they wish" (Cliff, Head, Brooklands). As Cliff noted Internet chat rooms allow individuals to conceal their identity, enabling adults to masquerade as children. The implied danger is that child sex offenders might use chat-lines to "groom" students before enticing them to meet off-line. Jo, the ICT co-ordinator noted that the risk of on-line chat rooms came not just from paedophiles but also from others who chose to be abusive. She remarked that "it's not that the Internet is crawling with paedophiles, but there are a lot of abusive people on-line" (Jo, ICT co-ordinator).

Overall staff concern about on-line chat rooms in primary schools focused on a number of issues including students being persuaded to meet up with strangers, the possible offensive nature of the language used, adults masquerading as children and the written abuse that might be targeted at children. Common to all these concerns was that students in primary schools were perceived as been at risk in on-line chat rooms.

2.2 Secondary schools

In secondary schools this concern that students were potentially at risk in chat rooms was also apparent. Nevertheless, some staff were also anxious that students were engaging in highly sexualised conversations on-line.

At Canalside the staff were anxious about students engaging in sexual conversations using the school Internet. Wilf the head of IT declared "it's not acceptable, what some students get up to on chat-lines" (Wilf, IT Head, Canalside). Following incidents where students engaged in sexual conversations on-line, Wilf tried to fine the students for abusing the system. For legal reasons he was unable to carry out this threat, though this might have been fortuitous insofar as fining students for accessing unsuitable chat-lines could be seen as tantamount to forcing them to pay for on-line sex chats! It is notable that all the other staff interviewed at Canalside commented upon Wilf's attempt to stop students using chat rooms. Unlike Wilf these staff also noted that chat-lines

posed a potential danger in the form of the activities of abusive strangers. Nevertheless the staff tended to touch upon this issue in passing while focusing largely upon the topic of disruptive students engaging in sexual conversations on the web. Ralph, a design and technology teacher at Canalside, talking about student chat-line activity noted "it's bad for the school image, not to mention the waste of resources" (Ralph, design and technology teacher, Canalside). Other staff agreed. Trevor, a music teacher, Simon, a geography teacher, Maggy, an English teacher and Adele, a science teacher respectively labelled student use of chat rooms as "dodgy", " a waste of time", "just plain obscene" and "bad for the school".

At Dalehouse Zed, the ICT co-ordinator, related that while he was happy for students to use the chat-lines permitted by the Internet filter he still worried that "some of the unmoderated chat-lines leave the student open to abuse, bad language, that sort of thing" (Zed, ICT co-ordinator, Dalehouse). Despite this concern Zed outlined plans to turn the library into an after school cyber-cafe so that students and parents could "surf" and chat on-line. Dave, the ICT manager at Dalehouse, remarked that while abusive strangers on chat-lines could be a problem, the filtering software tended to limit access to moderated chat-lines which he regarded as safe. "Unsuitable" chat-lines according to Dave were those that were abusive or sexual in nature. Thus he explained:

> There are very few chat-lines that they [the students] can actually get on, because of the filters. Hopefully what we call unsuitable chat-lines are filtered out. If they {the students] come across one that we think is unsuitable then it's only a matter of one phone call to get it taken off within an hour (Dave, ICT manager, Dalehouse).

At Eastway Mary declared that she was worried about student use of chat-lines while accepting that there was little she could do to stop it. She made the distinction that while younger students could be at risk from abusive language in chat rooms, the older students might be wilfully engaging in abusive and sexual conversations. Thus Mary remarked:

> With the younger students you worry they'll come across language they shouldn't be exposed to ... [laughs] The older ones [unintelligible] they're probably the source of these conversations (Mary, IT Head, Eastway).

At Forestfields Kate, the ICT co-ordinator, noted that "chat-lines are a worry because you never know who the students might be talking to" (Kate, ICT co-ordinator, Forestfields). While noting that chat-line use was banned in school, blocked by filter software and that students were always watched on-line, she still expressed concern that students might be subjected to abusive language or even attempts at seduction. Indeed Kate anxiously commented that "you read about it, adults enticing children into meetings and then abusing them" (Kate, ICT co-ordinator, Forestfields).

At Greenswold Robert, the ICT manager, explained that chat-lines worried him more than any other potential Internet risk. While he was bothered about students misusing the school resources, he also expressed concern about possible physical abuse if students were persuaded to meet strangers off-line. Furthermore he recognised the repercussions that such incidents could have for the institutions involved. He remarked that:

> It's going to happen somewhere eventually, it's going to happen isn't it. Some kid's going to get enticed out by the chat room whatever and something horrible is going to happen and the school will be blamed. I predict that now. I just hope it's not this one. But somewhere, sometime it will happen (Robert, ICT manager, Greenswold).

Arguably, this prediction, that students will be lured into meeting strangers and abused, lies at the heart of many teachers' concerns about student using chat-lines. Certainly all the other staff interviewed at Greenswold expressed concern about this possibility. Indeed Barry, the Head of science, Beth, a business studies teacher, and Hannah a geography teacher discussed the dangers of chat-lines solely in terms of the abuse that students might suffer. Karen, a geography and PE teacher and Colin, a history teacher, did also mention that students abused the school Internet by engaging in "unsuitable" on-line conversations.

Overall concern about the use of on-line chat rooms in secondary schools focused both upon the student being at risk and dangerous. Only Wilf, the IT Head at Canalside described student activities in chat rooms purely in terms of the deliberate mischief that they could cause. Rather nine staff described students as being both possible victims and sources of the dangers of on-line chat rooms. Six secondary school staff saw students solely in terms of being at risk from Internet chat rooms.

2.2 Post-16 Institution

The staff interviewed at Hightree expressed concern about the nature of on-line conversations that students were having. Tony related that "we noticed what I would term very unsuitable language and very unsuitable topics of conversation. They were frankly obscene" (Tony, ICT manager, Hightree). Jim, the Head of science remarked that "we're not a cyber-cafe and we're certainly not an on-line dating service" (Jim, Head of science, Hightree). These sentiments were shared by Alan, an English teacher, and Helena, a librarian, who respectively declared that some of the student on-line conversations "reflect badly on the college" (Alan, English teacher, Hightree) and were "just unsuitable in a place of learning" (Helena, librarian, Hightree). In addition to expressing concern about the effect that student on-line sex chats might have on the college image Tony also recognised that there was a more sinister risk. Indeed discussing chat-line use he declared that "students could be arranging to meet people, giving out addresses and telephone numbers. They could be putting themselves in danger" (Tony, ICT manager, Hightree).

Tony was the only member of staff interviewed to raise the concern that student might "flame" dignitaries, that is send abusive messages, using college e-mail accounts that had the institutional identity attached. Fretting about the damage that such activity might do to the college reputation Tony reflected that:

> I can't just sort of throw the [e-mail] accounts out individually, an account which has our identity attached to it. I just hope too many people don't start e-mailing Cabinet ministers or other personalities with insults... We're going to get some of those I'm quite convinced of that (Tony, ICT manager, Hightree).

It should be noted that while Tony pondered about releasing e-mail accounts with the school identity attached students accessed and used commercial e-mail servers such as MSN Hotmail.

2.4 Summary

In conclusion I would argue that there was an evident concern amongst staff about the possible dangers which children faced in on-line chat rooms. Fourteen staff expressed disquiet at potential student abuses of the net. Of these fourteen staff ten also articulated concern that the students were in danger. Ten staff were solely concerned that students were at risk. In common with their views of the dangers of Internet pornography the staff in primary schools who expressed concern about chat-lines saw the students as being solely at risk. In the post-primary institutions staff discussion of chat-lines tended to invoke the "dangerous student" image less than in their consideration of on-line pornography.

3. Hate engendering sites

Three staff, the ICT co-ordinator at Brooklands, a history teacher at Greenswold and the ICT manager at Hightree considered the possible detrimental effects of websites promoting hateful attitudes. In the case of Jo, the Brooklands ICT co-ordinator, the discussion focussed upon hate engendering sites that targeted teen pop icons such as the band S Club 7 (e.g. "Death to S Club 7") and Britney Spears (e.g. "Britney - Hit Her One More Time"). Jo noted that "the students are starting to realise that its people's opinions that are put on the net, but it can be a problem with the younger students" (Jo, ICT co-ordinator, Brooklands). She explained how problematically younger students might simply adopt the hateful attitudes presented on the "net" without questioning them.

Colin a history teacher at Greenswold related how in a lesson some sixth form students discovered a website that blamed Jewish doctors for the creation of "Gulf War syndrome".

> It [the website] had all tanks and people being injected, superb graphics. It just blamed "Gulf War Syndrome" on Jewish Doctors. It was superb the way they did it. And so somebody reading it might have thought that's true. A-level students can see it as propaganda whereas if you did it with year nine they might believe it (Colin, history teacher, Greenswold).

Jo and Colin's concern revolved around younger students being unable to critically interpret the information on hate engendering sites and correctly label it as vitriolic propaganda. Both teachers expressed concern that students might unquestioningly accept these hateful views, particularly if the websites were visually impressive.

Tony, the ICT manager at Hightree, pointed out that unless specifically blocked it was likely that many "hate sites" would get past the filtering software. Indeed he noted "It could be a bomb shell, put in a search for Nazi history sites and get informative academic resources, side by side with race hate material" (Tony, ICT manager, Hightree). This possibility is particularly disturbing when one notes the professional pseudo-academic presentation of some Historical Revisionist websites denying the occurrence of the Holocaust.

3.1 Summary

Concern about hate engendering sites was an issue touched upon by only three staff in total, one in a primary school, one in a secondary school and one in a post-16 institution. Anxiety about "hate sites" was clearly focused upon students being negatively influenced by inaccurate and hateful on-line propaganda. There was no suggestion that students might deliberately seek out such sites or even construct their own hateful websites. In this context anxiety about the hazards of hate engendering sites can be perceived solely in terms of the student being at risk.

4. Websites encouraging experimentation

With regards to other types of unsuitable on-line material, Wilf, the Head of IT at Canalside, mentioned the dangers of bomb making web sites, and Dave, the ICT

manager at Dalehouse, expressed anxiety about drug related sites. Their main concerns were that students would be physically hurt building bombs or trying narcotics.

According to Wilf the risk of students accessing bomb-making sites was that they "think oh this'll be a laugh, try and follow the instructions. It's just very dangerous eventually someone will end up dead" (Wilf, IT Head, Canalside). Dave noted that "a kid found a site on cannabis, it was quite educational. But obviously the worry is that it persuades the kids to try drugs. The physical risk could be very real" (Dave, ICT manager, Dalehouse). I suggested to Dave that some websites might contain "recipes" for individuals to develop their own narcotics using everyday substances. Dave remarked "I hadn't really considered that, but now you mention it I see that could be a problem" (Dave, ICT manager, Dalehouse).

4.1 Summary

In both of the above discussions the students were perceived as being physically at risk. Neither of the staff who touched upon the subject of websites encouraging experimentation expressed concern about how such incidents might reflect upon the school. Yet arguably students experimenting with explosives or drugs are dangerous insofar as they place not only themselves but also possibly friends "at risk". Despite this possibility both Wilf and Dave talked about the students in terms of them being at risk rather than dangerous.

5. Copyright

Overall seven of the staff interviewed expressed concern that the school might be at risk of legal prosecution arising from copyright infringement. Importantly staff did not always see students as intentionally breaking copyright law. Hence although their activities posed a legal risk to the school students were not always labelled as dangerous. Students intentionally downloading pirated music files from the web can be seen as an exception, as in this case they were perceived as deliberately posing a legal danger to the school.

5.1 Primary schools

The ICT co-ordinators at Avenue and Brooklands primary schools seemed particularly sensitive to the issue of copyright violation. This might reflect that they were both aware of staff who used a range of web-based material that was subject copyright in their teaching. Jo, the ICT co-ordinator sought to justify incidents of copyright violation by explaining that:

> I'm sort of under the impression that if the children take them [copyright material] and produce one copy for themselves, sort of put it into their own work then that's sort of acceptable. But I suppose it's still an issue [laughs] especially if we get sued (Jo, ICT co-ordinator, Brooklands).

Ella, the ICT co-ordinator at Avenue, stated that although the school might be violating copyright on material taken from the web, she understood that as long as they didn't make a profit from it then they would not be prosecuted. She further argued that it was difficult to control students copying material from the Internet, arguing "you can't restrict young children if they want to take a picture, they take a picture and it is on our website ... Maybe we should be more concerned" (Ella, ICT co-ordinator, Avenue).

5.2 Secondary schools

In the secondary schools concern about the legal risks of copyright violation of web-based material focused not so much on pictures, or print but rather on music files. ICT staff, including, Dave at Dalehouse, Mary at Eastway and Kate at Forestfields expressed concern towards the end of the research process that students were leaving the school open to the legal risk of copyright infringement by downloading pirated MP3 music files. Perhaps unsurprisingly, staff concerns increased after a high profile incident in the US where the music industry had threatened to sue an educational establishment for allowing students to download pirated copies of songs.

Only Kent, an art teacher and union representative at Eastway raised the issue of staff themselves being at risk from prosecution for copyright violation remarking

that "staff are legally responsible for their own plagiarism. That's a problem if you find something useful on the Internet but can't locate it's original source" (Kent, art teacher, Eastway).

5.3 Post-16 institution

Violating copyright on pirated on-line music was also a concern at Hightree. Tony, the ICT manager at Hightree, stated:

> One of the things I do try and block at the moment is downloading music. Now the problem with that for me is there are licensing issues, which of course the students are not interested in (Tony, ICT manager, Hightree).

Although unsure of the source of the information Tony believed that students downloading pirated music files via the college Internet could leave the institution open to a fine of £5,000.

5.4 Summary

Overall students tended to be seen as dangerous by staff when they deliberately sought to violate copyright by downloading pirated music files from the Internet onto the school system. However there was some sympathy for staff and students who unwittingly violated copyright or did so with the understanding that they would not be prosecuted. While students downloading pirated music was a concern in the secondary and sixth form institutions staff in the primary schools were unconcerned about this issue.

6. Security

Related to the students accessing inappropriate material were concerns with the school network security. Of the thirty staff interviewed nine expressed worries about security aspects of the school network. None of the nine teachers who expressed anxiety about security actually mentioned the risk of outsiders attempting to "hack" into the school system. Rather the focus was upon students abusing the system from inside the institution. These attitudes can be seen partly

as a response to certain incidents such as the swapping of passwords, "hacking" into the school network and attempts to gain access to the system administrator's account.

6.1 Primary schools

In the primary schools little concern was expressed about students "hacking" into the school systems. It can be assumed that this at least partly reflected the age of the students and their relative lack of technical knowledge of computer networks. However, at Brooklands Jo related how she discovered a boy accessing the *Simpsons* website using his older sister's password. This incident highlighted how a password security system installed to restrict access can be easily by-passed by a child. Talking about the incident Jo said, "It was a one off incident. But I would worry if it happened again" (Jo, ICT co-ordinator, Brooklands).

6.2 Secondary schools

At Canalside Wilf, the Head of IT, was concerned about students swapping or stealing one another's passwords. He argued that this created a network security problem insofar as students could side-step accountability for their "surfing" activities by using someone else's account or even claiming that someone else had used their password. In particular Wilf was concerned about students adopting such strategies when accessing pornographic material or adult orientated chat-lines. He remarked that students might be more willing to search for pornography or access adult chat sites if they were using someone else's password. While in a sense this didn't threaten the integrity of the school network it did create problems regarding accountability and the privacy of information stored on the hard drive. Simon a geography teacher at Canalside also expressed concern about the security risk presented by the Internet:

> Sooner or later something will be on the system which will be accessed by our students. Names and addresses of staff, data on kids whatever ... Sooner or later there's going to be a data protection issue there. Now we don't use the Internet at all for anything like that but we do use the school system and presumably if they [students] could get round it to access data, sooner or later

> they'll be able to access it through the Internet perhaps (Simon, geography teacher, Canalside).

For Simon the threat to school Internet security lay not outside, but rather was an internal one. Thus he feared that students might "hack" into the system and retrieve personal information, such as staff addresses. Yet it was not just information on teachers which Simon feared would be illicitly accessed, but also the private details of students. In this sense both students and staff were at "risk" of personal information becoming public knowledge. Although Simon initially described the potential perpetrator of these offences as student "hackers" he also considered the possible danger of staff abusing their position.

> As well I'm a bit concerned about staff e-mail. The security of that full stop. Because in theory the technician has access to all our pass words. And you know it's not unknown for people to do things ... I'm not saying anything about this school, but issues can come about (Simon, geography teacher, Canalside).

During the research this was the only statement made by a member of staff that allowed for the possibility that fellow staff might actually pose a risk to others. In this case Simon noted the potential for ICT staff to abuse their power.

At Dalehouse, Dave the ICT manager, related how his primary concern was not students accessing pornography or adult chat-sites but rather attempting to "hack" into the school system. Thus when discussing various examples of misuse of the school Internet which had occurred he claimed that "the ultimate [punishment] is that we'd withdraw access to the whole of the school network. That would be for something like getting on the file server" (Dave, ICT manager, Dalehouse). When asked why security was such a concern Dave responded "well it's the damage they could do. That's not to mention the restricted information we hold on there" (Dave, ICT manager, Dalehouse).

At Eastway Mary, the Head of IT, became concerned about security issues after a group of sixth formers managed to "hack" into the school network. Mary was upset that students had been able to access prohibited information on staff peer reviews and papers for forthcoming internal exams. She labelled the students

responsible as "tossers" arguing that their activities were "as bad as going into the staff room and stealing papers" (Mary, IT Head, Eastway). The possibility that these activities might re-occur was one that Mary took seriously, "our system isn't bullet-proof. I'm just worried students will take advantage of that fact. Getting information that might embarrass staff or create more work for us" (Mary, IT Head, Eastway).

Concern with students swapping passwords was evident at Forestfields. Kate, the ICT co-ordinator at Forestfields, commented that "the main worry we had was the security aspect ... students telling each other their passwords and going on to each others' files" (Kate, ICT co-ordinator, Forestfields). She explained that this was problematic in that students accessing one another's account could alter or delete work stored on the hard drive.

Robert, the ICT manager at Greenswold, was concerned about the security of the school network because it acted as a gateway to the World Wide Web for local primary schools. Any internal breach in system security would not only affect students in Greenswold but also students in local primary schools. In particular Robert was concerned about Greenswold students placing unsuitable material on the school network that they might have downloaded from their home Internet. Thus he observed, "the nightmare scenario is that some of the stuff gets into our cache and a primary school kid mistypes an address and up comes this pornography" (Robert, ICT manager, Greenswold).

6.3 Post-16 Institution

At Hightree Tony, the ICT manager, and Jim, the Head of science expressed concern about internal security issues. Tony related that while he wanted to make the system accessible to other teachers and technical staff he was concerned about students being able to take advantage of weaknesses in the network. In discussing some of the student attempts to alter the pre-sets on the system Tony complained about a particular student, "this very well known hacker he's caused me a lot of pain in the past ... he's a pain in the neck at the moment, always

trying it on" (Tony, ICT manager, Hightree). For both Tony and Jim the concern was that students would create more work for technical staff. Jim explained:

> We haven't got much information up and running on the school network, so that's not so much of a problem. It's more the students messing around trying to install their own programs, trying to alter the network. It's just more work (Jim, Head of science, Hightree).

Arguably staff concerns at Hightree may alter when information such as peer reviews and inspection reports become stored on the local computer network and potentially accessible to student "hackers".

6.4 Summary

Eight staff who expressed concern about Internet security did so in terms that constructed the students as a danger to system integrity. While Jo, the ICT co-ordinator at Brooklands primary school, was anxious about network security issues she did not describe related student activities as being threatening. Nevertheless, in the post-primary schools it was recognised that students might use passwords other than their own or claim that their password had been utilised by someone else in order to avoid punishment for accessing unsuitable on-line material. Despite staff awareness that students might steal one another's Internet passwords only Simon, a geography teacher at Canalside, and Kate, the ICT co-ordinator at Forestfields, explicitly reflected that this might put students at risk of having material altered or stolen. Simon was the only member of staff to consider that fellow employees might choose to abuse the network by accessing restricted information or using others' passwords. Overall concern about school network security in post-primary schools tended to focus on the student as a source of danger. Thus staff were anxious that students might access confidential on-line information, damage the network, create work for technical staff and post undesirable material on the system.

Conclusion

In drawing together the threads of the staff Internet risk narrative I will now review the main concerns whilst distinguishing between discourse focused on the "student-at-risk" and that relating to the "dangerous student". I will note that while in the primary schools students were seen solely as victims of Internet risks, in the post-16 institution the students who used the Internet were largely viewed as potential sources of danger. In secondary schools these narratives of the "student-at-risk" / "dangerous student" were both invoked.

The majority of staff interviewed were concerned about the dangers posed by on-line pornography. Thus twenty-eight staff voiced concern about this issue. With regards the accessing of on-line pornography, eighteen staff described the students as a source of danger, five considered the students as being solely at risk and three labelled the students both as potential victims and dangerous to the school. Two staff did not expand on their assertion that on-line pornography was a problem. The greatest concern of the twenty-eight staff who considered on-line pornography a problem was the threat it posed to the school image and staff authority. Only five staff saw students as being solely at risk and three of these respondents worked in primary schools. Indeed within primary schools three staff worried about sexual web content discussed it purely in terms of the student being at risk. The other primary school teacher interviewed did not consider on-line pornography a problem. In contrast all four teachers interviewed in the post-16 institution saw students accessing pornography solely in terms of the potential problems it might create for staff and the college. This lack of concern about the effects of pornography on the students was justified with reference to the age of the college students.

In total twenty-four of the staff interviewed were anxious about students using chat rooms. Ten staff focused solely on the threat to students from the activities of undesirable others. A further ten added that they thought students chatting on-line were not only in danger but also potentially put the school at risk. Four staff discussed student use of chat-lines entirely in terms of the threat posed to school image and resources. Within primary schools the four staff interviewed

considered students to be at risk in chat rooms, whereas in the post-16 institution three teachers argued that on-line chatting was a waste of resources and a threat to the college image. One member of staff from Hightree College while critical of the problems created by students using chat-lines also expressed concern about their safety.

Only three staff, one each from the primary, secondary and the post-16 sectors, expressed concern about hate engendering websites. All three acknowledged that the problem was more serious with younger, impressionable children. The staff who raised this subject saw students as being at risk from unquestioningly accepting hateful attitudes.

Two staff expressed concern about websites that sought to encourage experimentation. Wilf the IT Head at Canalside was worried about websites containing bomb making recipes, while Dave, the ICT manager at Dalehouse was anxious about websites promoting recreational drug use. Both Wilf and Dave saw students who might use such websites as being at risk. Neither teacher raised the issue that students could potentially pose a threat to others if they attempted to manufacture their own explosives or narcotics.

Of the seven teachers who discussed copyright violations, two primary school teachers were concerned about on-line material, four post-primary staff mentioned the issue of students downloading pirated music file, and one art teacher in an 11-18 institution was anxious about the legal risk to teachers. In primary schools staff did not perceive students who infringed on copyright as intentionally creating a legal risk. However, in the post-primary institutions students who downloaded pirated music files onto the school network were described as intentionally creating trouble.

Overall nine staff discussed the problems of school network security. Eight staff, all in post-primary institutions, concentrated on the dangers that student "hacking" activity posed to the schools in terms of the accessing of prohibited information and creating work. Two of these eight, Simon, a geography teacher at Canalside, and Kate, the ICT co-ordinator at Forestfields, also considered that

"hacking" might pose a threat to student work stored on-line. While Jo, the ICT co-ordinator at Brooklands primary school was worried about on-line security she did not describe students as a threat to network integrity. Thus it was only in the post-primary institutions that discussions about network security tended to invoke the narrative of the "dangerous student".

Overall the majority of teachers saw pornography and chat-lines as problems. While the concern about on-line pornography related mainly to the threat to school image, concerns for students using chat-lines was more balanced between the "student-at-risk" / "dangerous student" narratives. While copyright violation was a concern for some teachers, students were only described as creating risks insofar as they downloaded pirated music files onto the school system. Network security issues were seen as a problem by just under a third of the staff and such views tended to be couched almost entirely in terms of the "dangerous student". Few staff raised the issue of hate engendering sites or websites encouraging experimentation with explosives or drugs.

In conclusion it can be seen that with regard to a range of risks arising from the Internet primary school staff tended to perceive their students as being at risk. This was in contrast to the post-16 institution where staff saw students' misuse of the Internet largely as a source of potential danger. In secondary schools these narratives were more intertwined with Internet activity viewed variously as putting students at risk and creating danger for the schools.

Having considered staff perceptions of the risks arising from school Internet use I will concentrate in the following chapter on the student narrative. Thus I will consider the issues of pornography, chat-lines and security, before finally arguing that some students' activities hinted that they saw punishment for Internet misuse as a risk.

Chapter Five

Student perceptions of risks arising from school Internet use

Introduction

To suggest that students responded to the risks posed by Internet use in a uniform manner would be inaccurate. Indeed the peripheral nature of the "net" in the learning process in schools meant that, beyond some introductory sessions, students could avoid contact with it if they so wished. Early in the research process, I recognised the importance of detailing the Internet risk narratives of students. However, as will be argued, the spoken student narrative about Internet risks was sparse. While this might reflect a perception of the Internet as "non threatening" and "safe", I will argue that some students' behaviour indicated that some were concerned about being punished for misusing the school Internet.

Sixty-three students in total were interviewed (see table four for more details). In the primary schools the interviews tended to be informal involving students who were "surfing" the web, asking them about their current activities, how this related to general Internet use and what problems arose from using the school "net". Four students were interviewed at both Avenue and Brooklands. The majority of interviews in the post-primary schools were opportunistic and semi-structured. Eight students were interviewed at Canalside, Greenswold and Eastway, nine at Dalehouse. and Forestfields, and thirteen at Hightree. In addition to interviews, students were observed using the Internet during lessons, before and after school, in free periods and at lunchtime.

The most notable feature of the student risk narrative was its almost non-existence on a verbal level. While all sixty three students were asked about the problems and dangers that they perceived surrounding the Internet very few expressed concerns beyond the problems of web searches producing too many "hits", the pitch of websites and the reliability of on-line information. Indeed at Avenue, Brooklands, Dalehouse and Greenswold students did not express any concern about on-line dangers. I would argue that the failure of the students

interviewed in these four institutions to report any risks arising from school Internet reflected a genuine lack of anxiety about on-line hazards. However, I will argue that some students displayed non-verbal indicators of concern about punishment arising from school Internet misuse.

There was no discussion of race hate, bomb or drug making websites. Likewise, no mention was made of legal, financial or reputation risk. Rather the three issues that did emerge from the interviews related to risks arising from pornographic material, on-line chat sites and doubts about the security of the school system.

1. Pornography

Only eleven students touched upon the subject of Internet pornography, one at Canalside, three at Forestfields and seven at Hightree. Of these students, only two were concerned with the possibility that they might accidentally stumble across pornographic material. No student expressed concern about the potential negative psychological impact of viewing pornography, but three students at Hightree did discuss the negative effect accessing such material in college might have on the institutional reputation. In considering these narratives about on-line pornography in more detail I will, where appropriate, draw distinctions between "at risk" and "dangerous students". No primary school students in the research raised the issue of on-line pornography.

1.1 Secondary schools

At Canalside Phil, a year 10 student, went further than merely discussing the possible hazards of accessing on-line pornography. While describing the effectiveness of the filtering system, he typed "porn" into a search engine and said, "I'll show you. Let's hope it doesn't come up though. Sometimes it comes up and you just kind of hide it on the screen" (Phil, year 10, Canalside). Fortunately the filtering software was effective and the search was blocked. Arguably, Phil's recognition of the need to hide pornography indicates that he saw punishment for accessing it as a danger. Indeed earlier in the year he had

been banned from using the school Internet for a term after accessing a pornographic image.

At Forestfields students touched upon the issue of pornography on the "net" upon two separate occasions. The following discussion took place between two year eight girls being interviewed in the library:

> June: Do you know when you're allowed to use them [Internet machines] after school? Well John Smith [name changed], he used to go to my primary school, he was on the computer looking up disgusting porn sites
> Avril: I know all boys go on like naughty sites and the girls are just like just keen to learn.

This conversation took place, at a higher volume than the rest of the interview, with the girls staring at John Smith who was stood about four metres away. Both girls were smiling and it would be difficult to interpret the narrative as being an expression of real concern. Rather it seemed part of an interplay, with the girls attempting to taunt John. Avril's assertion that unsuitable sites are "naughty" is interesting insofar as it invokes narratives of misbehaviour.

In response to the question of whether he thought the Internet was useful, a year seven student at Forestfields replied "yeah but there's so many porn websites and stuff. Like if you type www.buffy.com it'll come up filtered and things like that" (Daniel, year seven, Forestfields). Daniel expressed concern that in attempting to build his school web page based on *Buffy the Vampire Slayer*, a popular teen television series, he might stumble across pornographic websites. This might be true insofar as "buff" is an Americanism for naked. Nevertheless, Daniel could not explicitly explain why he was worried that his web searches might expose him to pornographic material.

1.2 Post-16 institution

At Hightree, three students broached the subject of pornography in response to questions about activities prohibited by the school Internet Acceptable Use Policy. The three year twelve students two male and one female replied that

while they couldn't remember which activities the AUP restricted, they thought that "surfing" for pornography on the web was mentioned. When asked why they thought this was prohibited if they couldn't remember what the AUP covered they replied that it was "common knowledge" and "common sense". Further questioning about why they thought this activity was prohibited revealed that they all considered students accessing pornography to reflect badly on the institution. One of the students Saul argued "if we use the Internet to download stuff like porn, it's not so much that it's bad for us, but it reflects very badly on the college" (Saul, year 12, Hightree). Furthermore another member of the group, Judy, noted that "pornography might be bad for young children, sure, but we're adults" (Judy, year 12, Hightree). Thus the students dismissed the possible psychological affects that exposure to pornography might have on older student. Therefore, in discussing on-line pornography the students invoked the "dangerous student" narrative rather than the "student-at-risk" one.

Faye, a year 13 student at Hightree, mentioned that "if you like go on dirty sites [laughs] you get barred" (Faye, year 13, Hightree). When asked whether this put her off using the Internet, she noted "well it's not like I'd go to these sites, but with the Internet you never know where you end up. I just don't use it ... I don't know how to" (Faye, year 13, Hightree).

While no other students at Hightree expressed concern about stumbling upon pornographic websites, Tony the ICT manager had remarked that immediately following the punishment of a student for accessing a pornographic website, students' concern over stumbling across such sites notably increased. Tony related how "we found students coming knocking on the door saying I've accidentally got into somewhere that I didn't want to go into, but it happened. Will I be suspended for this?" (Tony, ICT manager, Hightree).

Three year 13 males at Hightree discussed in some detail the incident where a student accessed a picture of a naked woman on the FHM magazine website and was subsequently expelled. Yet, their concern was not with the potential dangers of pornography or the threat to the college image. Rather their consideration of on-line pornography focused entirely upon how magazine images that were not

considered pornographic or prohibited could be redefined as "porn" by staff when posted on the Internet. The students might be seen as complaining that they were at risk from the staff re-interpretation of material that was seen as broadly acceptable in the outside world. This incident is discussed at greater length in chapter six.

All seven students at Hightree who discussed on-line pornography did so with reference to the possibility of being banned from the Internet or expelled from college. None of the students drew upon the narrative which constructed the material as psychologically harmful or presenting a risk to themselves. Rather they described the danger of accessing such material as the possibility of punishment.

1.3 Summary

Overall only two students out of the sixty-three interviewed expressed concern that they might accidentally stumble across pornographic sites on the Internet. Yet, these two students, Faye at Hightree and Daniel at Forestfields, did not touch upon the possible harmful psychological affects of such material. Rather the subject of pornography seemed an occasional source of amusement. Thus June and Avril referred to "porn" in an apparent attempt to embarrass a boy, Faye at Hightree laughed as she mentioned "dirty sites" and Phil arguably saw it as providing an arena in which he could display his computer skills. Indeed student perception of risks from on-line pornography seemed to focus on punishment and the threat to the school reputation. Having considered the virtually non-existent expressions of student discomfort about on-line pornography I shall now examine student risk narratives regarding chat-lines.

2. Chat-lines

While the majority of students interviewed discussed chat-lines, only five students in total, two at Eastway and three at Hightree, touched upon the risks that they saw such sites as posing. All of these five students expressed concern about undesirable others in on-line chat rooms. Although primary school students

in the research mentioned chat-lines, they did not raise the issue of risks. This might reflect innocence about the dangers, as well as the fact that they were not allowed to, and reportedly did not, access such websites.

2.1 Secondary schools

At Eastway, two students mentioned dangers that they thought existed in on-line chat rooms. Larry, a year ten student at Eastway expressed anxiety that individuals could lie about their age and identity on-line. Despite his worry that in chat rooms "you never know if their age or sex is a lie" (Larry, year ten, Eastway) he admitted to telling others that he was twenty-one years old and upon one occasion masquerading as a girl on-line. The sense of risk that Larry expressed was unfocused. He never managed to explain why people lying about age or their sex bothered him, especially as he did it himself. More direct was another year 10 student at Eastway, who linked his concerns firmly with the reported activities of paedophiles on-line. Although focussing on Internet access at home rather than at school, in response to the question of whether he went on chat sites he replied, "[n]ot any more. I used to. Now all these risks have come out, other people getting on the other end ... Just about paedophiles and things getting on the other end" (Robin, year ten, Eastway). While Robin expressed concern about paedophiles on-line, he admitted that he still occasionally accessed chat rooms. This begged the question of how anxious Robin was about such risks.

2.2 Post-16 institution

At Hightree three students expressed concern about the dangers of chat rooms. Complaining that too many people asked personal questions on chat sites, Alex a year 12 student, explained how he had been 'hassled' by a person he had communicated with in a chat room. Reportedly the man insisted on sending Alex silly messages and requests to meet up. While the solution to the problem was simply to ask the message providers to block communications this incident nevertheless indicated how students could be harassed in cyber-space. Two year thirteen students, a male and a female, respectively described on-line chatters as

"screwy" and "creeps". Although the year thirteen male, Will, did admit to exchanging e-mail addresses and messages with people he met in chat rooms he noted that "it never lasts, a couple of e-mails and that's it. They're usually far too screwy" (Will, year 13, Hightree).

2.3 Summary

Overall only five out of the sixty-three students interviewed expressed concern about the dangers that were seen as lurking in on-line chat rooms. More students who discussed chat rooms were positive about what they saw as the benefits. According to the ICT manager at Hightree one girl told him that she thought chat rooms were a "rite of passage". Two year eight students at Forestfields, June and Avril, related how they had slumber parties where they and their friends would access chat rooms and "compare your problems with their [other on-line users] problems" (Avril, year eight, Forestfields). A year ten student at Greenswold mentioned how he met his girlfriend, who lived over forty miles away, through a Formula One motor racing website. Another Greenswold student explained that he felt it was easier to strike up a conversation with people on-line rather than face to face. This year 11 student was particularly interested in cross-country cycling, had ordered his bike over the web, and interestingly had a chat room persona named Pashley, after the brand name of his bike.

Despite chat-lines being prohibited in Avenue, Brooklands, Canalside, Eastway, Forestfields, Greenswold and Hightree, students didn't appear overly concerned about the punishments arising from any transgressions. This might reflect the minor punishments and the common occurrence of students being caught using the school Internet to access chat rooms in post-primary schools. At Eastway, Greenswold and Hightree students were observed being told to log off and leave the room when caught on chat-lines by staff. In these cases, I would argue that there was little student perception of chat-line use as being dangerous to the institution. Rather if any risk did exist it was embodied in the "screwy" individuals on-line. However as Alex noted undesirable individuals could easily be blocked and the student could always withdraw from cyberspace. Ultimately

whatever risk was offered by undesirables on-line could be easily avoided by students if they so wished.

In conclusion it can be noted that while younger students had little to say about the risk offered by strangers in chat rooms, these are the ones that have been identified in the media as being potentially the most vulnerable. Having considered student risk narratives about Internet chat-lines I shall now focus on the issue of security.

3. Security

Despite the swapping of student passwords, the ability of staff to snoop on-line, or students engaging in e-commerce using the school "net" only three students, one at Eastway and two at Hightree, expressed any concerns about Internet security in school. None of the primary school children interviewed raised the issue of security.

3.1 Secondary school

The only student who directly discussed the issue of network security and the school Internet was concerned about protecting the school system from "hackers". Perhaps it is unsurprising that the year ten girl, Kelly, who expressed anxiety about the school system being "hacked" was a student at Eastway, where a group of sixth formers had managed to gain access to restricted areas on the school Intranet. As Kelly argued "well I mean there is (sic) a few computer whiz kids and people can do things to computers, like put bugs and everything in" (Kelly, year ten, Eastway). Thus Kelly was concerned about the risk posed by "hackers" to the school network. Although it should be noted that she did not distinguish between internal and external threats to the system. Therefore uncertainty existed as to whether Kelly was expressing concern about the "dangerous student" or rather "hackers" who were outside the institution.

3.2 Post-16 institution

Will, a year 13 student at Hightree, explained that while he had bought items on-line using the Internet at home, he wouldn't use the school Internet to make such purchases. The reason he gave was that:

> I think it'd be less secure. The teachers ... I know they wouldn't sort of nick it [credit card number], but they have access to everything we've done on here [the school Internet]. And if they have access then somebody else is bound to be able to" (Will, year 13, Hightree).

For Will this belief that staff could view his financial transactions if he used the school Internet rendered the system effectively insecure. Tony, the ICT manager at Hightree, dismissed this claim that he could gain access to credit card numbers on the school Internet. Other students seemed not to share Will's concern. Indeed of those interviewed eleven students, one at Dalehouse, one at Greenswold and nine at Hightree, admitted to buying products using the school Internet.

One year 12 female student at Hightree initially objected to the idea that the school might read her personal e-mails. She subsequently changed her mind saying that she'd probably forget that that her messages were being read.

3.3 Summary

Overall only one student interviewed, Kelly at Eastway, expressed concern about risks to the institution from on-line "hackers". The thought that staff might be able to access information students had placed in their own computer accounts caused little concern. This might be understood in a context where students swapped passwords with one another. As with the issues of pornography and chat-lines, there appeared to be little student concern about security. While maintaining that students were not overly concerned about the Internet risks that were a source of anxiety for staff, I will now argue that students were actually worried about being punished for inappropriate Internet use.

4. Punishment

In the post-primary institutions included in the research there was an evident non-vocal discourse which suggested that students were concerned about punishment. I would argue that these concerns should not be strictly regarded as risks, as with the exception of one student, who was expelled, there were few serious outcomes arising from punishment for on-line behaviour. Nevertheless, I would maintain that the concern that students displayed regarding punishment for deliberately misusing the school Internet should be briefly considered. Only Faye a year 13 student at Hightree explicitly expressed concerns that accidentally accessing inappropriate websites might lead to castigation. There was no evidence that suggested that fear of punishment for inappropriate on-line activities resulted in students shunning the Internet.

Insofar as I am seeking to make no claims beyond asserting that some students were worried about punishment for deliberate on-line misdemeanours, I will not provide a detailed account from each school involved in the research process. Rather I will highlight certain incidents in schools that I believe illustrated students' concerns about the possibility of punishment for inappropriate Internet use. The physical and virtual surveillance measures adopted by the schools in this research are considered in detail in chapter eleven.

Students were observed engaging in a wide range of activities that could be viewed as attempts to avoid staff surveillance and punishment. In the schools studied punishment included verbal harassment by staff, students being thrown off the Internet, the withdrawal of Internet access, calling the students' parents into school or even in one case expulsion. At least partly to evade such punishments students sought to counter physical surveillance of on-line activity. Thus students hid monitor screens, adjusted consoles so that the screens could not easily be seen by observers, purposely chose Internet machines in secluded corners, hid web pages behind acceptable work, used other students' passwords, waited for unsupervised "windows of opportunity" to misuse the Internet and maintained their own surveillance of members of staff and other students who might object to their Internet misuse. Additionally in seeking to avoid

punishment for Internet misuse students engaged in activities that allowed them to render virtual surveillance packages ineffective. Hence students swapped, stole and claimed that others students had used their Internet passwords. They also accessed unsuitable websites whose innocuous on-line addresses did not alert staff as to the true nature of the site. I will now consider in turn the strategies of both physical and virtual concealment, which some students adopted to avoid punishment for inappropriate use of the school Internet.

4.1 Physical concealment

In considering student practices of physically concealing inappropriate Internet use I will examine issues of screen visibility, monitor adjustment and the positioning of personal computers. Additionally I will contemplate student attempts to hide material within windows on the monitor screen and the speed at which students concealed items on-screen. Finally I will draw attention to how some students attempted to use different Internet locations and time periods to hide their on-line activities.

Some attempts at blocking screen visibility were counter productive in that they drew attention to Internet misuse. Thus at Canalside I saw students obscuring computer screens with hands and books in an attempt to hide their offensive e-mails. At Dalehouse I observed students blocking an unsuitable on-screen image by standing in front of the monitor. However in both these cases the overt nature of the concealment soon attracted attention. This raised the question of whether the students seriously intended their "blocking" activities to be effective strategies for avoiding detection. Indeed the students at Canalside appeared to be primarily concerned with blocking the view of the neighbouring students to whom they were sending the offensive e-mails, while those at Dalehouse seemed eager to gather around the monitor so that they could view the image of a scantily clad female wrestler.

A more covert form of screen concealment utilised by students was adjusting the position of the monitor in an attempt to reduce the screen visibility for others. In all post-primary institutions students were observed engaging in this activity,

which normally involved turning the monitor screen towards the nearest wall, as opposed to aligning the screen with their own sitting position. At Canalside, Phil a year 10 student, explained how he normally selected a computer that was on the end of a row, nearest the wall, so that he could turn the screen towards the wall to restrict staff view of it. A female sixth form student at Greenswold sending an e-mail that started with the line "Hello Sexy" adjusted the screen position so that it pointed away from the librarian who was sitting at a neighbouring computer. Later while chatting, this girl expressed the opinion that:

> Well I don't want people to read my e-mail, but I guess it bothers me more if teachers do. My friends don't bother me, but teachers do, after all I could get into trouble (Elizabeth, year 12, Greenswold).

At Hightree students playing games on the Internet were observed turning the screen away from positions in the room occupied by staff.

Students who sought to adjust the angle of their computer monitor to make it more difficult to observe sometimes chose an Internet machine whose screen was difficult to see from other positions in a room. The monitors of computers in corners could be slightly adjusted to face towards the wall, which made the screen difficult to view from the centre of the room. At Eastway it was noted by the ICT technician that a sixth form student who had "hacked" into the staff network had used an Internet machine that was located at the back of the room, positioned in such a way as to make the screen virtually impossible to see from anywhere else in the ICT suite. Discussing concealment of screens, Ben, a year 13 student at Hightree, remarked that "[i]t's easier if you're at the bottom two", pointing to the Internet machines in the corner "or those two" pointing to machines at the opposite end of the room again in the corner. It was difficult to see the screens of the computers indicated by Ben unless you squeezed in behind the students using them. The computers pointed out by Ben were the ones that Tony, the ICT manager at Hightree, claimed students favoured when misusing the Internet.

In addition to attempting to restrict visibility of the actual console screens students also resorted to hiding webpages within screens, either by overlaying

them with other pages, or by minimising the size of the offending webpages. At Canalside, Phil, a year ten student, provided an insight into how students could conceal what they were actually accessing on the Internet. He showed me how if teachers were to approach him he could click on the minimise icons on webpages, hiding any offending material in the tool bar at the bottom of the screen. When asked whether he thought he would be able effectively observe other students' Internet activities he pointed at the tool bar at the bottom of the screen and replied:

> I'd just come round and look at the bottom of the screen. That [tool bar symbol] means the Internet, that means files. You can tell by the symbols on the bottom, that's what I'd do (Phil, year ten, Canalside).

At Eastway following a breach in Intranet security, Mary the ICT Head, discovered that a student logged onto a machine in the library was attempting to use "hacking" software. She was able to identify which student it was by checking his username, and headed off to the library intent not on confrontation but rather on surveillance. After ten minutes in the library watching the student, and even briefly chatting to him, she returned to the technicians' office reporting that she had seen nothing incriminating. One of the technicians informed her that the "hacking" programme had been open all the time she had been in the library, and they both agreed that the student had hidden it behind other windows on the screen. As Robert the ICT manager at Greenswold explained "there is a minor problem and that is students having stuff running in the background but that's just kids being kids ... Sometimes its a bit difficult, kids are very good at it" (Robert, ICT manager, Greenswold). While discussing the issue of concealment with Ben and Bill two sixth form students at Hightree, Ben illustrated the ease with which items could be hidden on the computer screen. He closed a word processing document that was occupying the screen, behind it was revealed a window from an on-line chat site. When asked why students hid such webpages Ben replied "well we're not supposed to go on chat sites, but it's ok as long as we don't get caught. Doing this means we won't get thrown off [the Internet]" (Ben, year 13, Hightree).

In all post-primary schools, staff expressed concern at the speed at which students were able to exit unsuitable webpages. One geography teacher at Greenswold noted that this speed of reaction made it very difficult to actually see what students were accessing, "[t]hey're so quick. They're clicking the screen off as you walk past. You know they've got everything sussed" (Hannah, geography teacher, Greenswold). Phil a year ten student at Canalside showed how he could log off the system almost instantaneously by pressing four keys in sequence. Indeed the practice of concealment was made more effective by the speed at which both the students and the computer systems operated. At Canalside students were observed playing games on the web during lunchtime. This was a banned activity so whenever a member of staff approached them, the students would quickly hide the game and pretend to be engaged in legitimate work. When the staff member moved away the student would go back to the game. Occasionally a student wasn't quick enough and got caught and thrown off the computer. In some bizarre manner this interaction between staff and students had many of the qualities of the games that were been played on-line, requiring alertness and speed of response.

It was noted that lower levels of physical surveillance of Internet use existed in certain locations. Thus Internet computers in sixth form areas were rarely the subject of staff observation. John, a year thirteen IT student at Forestfields, recognised that in certain locations staff physical surveillance of on-line activity was virtually non-existent. Thus he noted:

> We can mess around on the Internet in the sixth form area because we're left largely unsupervised. Here [the Learning Resource Centre] you're constantly watched so if you mess around, you'll just get thrown off the computer by the librarian (John, year 13, Forestfields).

Robert, the ICT manager at Greenswold, had formally objected when the Head decided to place Internet machines in the sixth form base, arguing that students given unsupervised access would be more likely to misuse the "net".

Not only were certain locations perceived as being subject to lower levels of physical surveillance, but the issue of timing was also important. For example at

Eastway one student who was caught accessing another students' computer account had waited until after the end of the school day to commit the act. Over the course of a week at Forestfields I observed three year eight students using the Internet in the Learning Resource Centre. Their Internet use was deemed broadly acceptable by the staff and student monitors who watched their on-line activity. However on Friday evening when the LRC was unsupervised the three students were seen exploring a site called *Poo III*, a website featuring verse and pictures dedicated to defecation. This illustrated how students might wait for windows of opportunity in which they could misuse the Internet without been observed by staff and subsequently punished.

4.2 Virtual concealment

There was an awareness amongst students that the identification tag of a username combined with the logging of the addresses of web sites visited, enabled staff to reconstruct a picture of sites that students had visited using the school Internet. To avoid such measures of accountability students swapped, stole and claimed that others had used their Internet passwords. Furthermore in an attempt to avoid virtual detection and hence punishment students also sought unsuitable websites which had innocuous on-line addresses.

Phil, a year ten student at Canalside related how his friend had given him someone else's password. He noted "I used that if I wanted to do something daft, so I didn't get caught out" (Phil, year ten, Canalside). Indeed Phil claimed to know almost fifty student passwords. Simon a geography teacher at Canalside noted that one outcome of students swapping and using one another's Internet passwords was that they "could always claim that their password was given to someone else" (Simon, geography teacher, Canalside). Indeed Simon described how some students confronted by Wilf, the IT Head, with evidence of Internet misuse had claimed that other students had stolen and used their passwords. Reportedly both Wilf and Simon saw such claims as attempts to avoid punishment by students who had misused the school Internet.

At Forestfields John, a year 13 student, discussed how students could get round the school filtering system by accessing sites where blocked terms were misspelled. He also noted that some adult websites used innocuous web addresses, remarking that "you can always find dubious sites with innocent names. They won't attract any attention when logged" (John, year 13, Forestfields).

4.3 Summary

In exploring attempts at concealing on-line activities I have shown that some students were concerned about punishment for inappropriate Internet use and tried to avoid surveillance. Thus I highlighted some examples where students engaged in activities of physical and virtual concealment in an attempt to avoid punishment for school Internet misuse. With regard to physical surveillance of the Internet I considered issues of screen visibility, monitor adjustment, computer positioning, hiding material on-screen and choosing locations as well as times that were subject to lower levels of surveillance. Focusing upon student attempts to avoid virtual surveillance of on-line activity I briefly examined the practices of swapping, stealing or claiming that someone else had used an Internet password and students accessing inappropriate websites which had innocuous on-line addresses. In conclusion I do not seek to make any claims beyond asserting that some students were worried about punishment for on-line misdemeanours and attempted to conceal such misuse.

Conclusion

Overall there was a somewhat limited spoken student risk narrative, focusing on pornography, chat rooms, and network security. Unlike the staff who were interviewed students expressed no concern about bomb making, drug related or hateful websites. No mention was made of plagiarism, libel or copyright laws. There was no evidence to suggest that students saw the Internet as a threat to their status. Rather for some students, such as Phil at Canalside, the Internet offered a showcase for technical talent.

While eleven students discussed the problem of on-line pornography, only two of these were concerned that they might accidentally stumble across such material while using the school Internet. One of these students, Faye (year 12, Hightree), did not appear to be worried about the effect of the actual material but rather was concerned that she would be thrown off the Internet, while the other student, Daniel (year 7, Forestfields), was unable to explain why he was anxious. There was no indication that either student saw him or herself as being at risk from on-line pornography. Indeed three other students, all at Hightree, invoked the "dangerous student" narrative when remarking that accessing pornography on the school Internet reflected badly on the institution.

Although the majority of students interviewed touched upon the subject of chat-lines only five students labelled them as "risky". One of these students, Alex a year 12 student at Hightree, noted that while he had been harassed on-line the solution was simply to ask the cyber-chat provider to block messages from the individual. Overall, students seemed quite positive about using chat-lines, even though they were banned in all institutions except Dalehouse. Indeed, one student at Hightree was reported to have labelled the use of chat-lines on the school Internet as a "rite of passage".

Three students expressed concern about security issues relating to the school Internet. While one student was worried that if he bought items over the school Internet his credit card number would be stolen, another was initially concerned with staff reading her e-mails. Only one student was directly worried about the threat to the school network posed by "hackers".

While the verbal student Internet risk narrative was somewhat limited, students adopted techniques that could be broadly labelled as attempts to avoid punishment for misusing the school Internet. Thus they hid computer screens, adjusted monitors, hid windows within screens, used other students' passwords and selected places / times when staff surveillance was sparse or absent. Additionally students swapped or stole passwords and accessed inappropriate websites that had innocuous titles. I argued that punishment for Internet use

could not be seen as a risk insofar as it was rarely sufficiently serious to offer a real threat to the students.

In conclusion, I would note that students verbally expressed little concern about potential Internet risks. Indeed the vast majority of students interviewed were either unconcerned or unaware of possible on-line threats to themselves or the institution. While four students did consider how the school might suffer from students accessing pornography or "hacking" into the network overall there was little reported student concern about the possible risks to the institution arising from school Internet use. This lack of concern was even more pronounced in the primary schools where, despite direct questions about negative aspects of the web, no single student raised any concern about the Internet. Indeed this attitude was reflected in Dalehouse and Greenswold where students largely had positive things to say about the school Internet.

Following consideration of the staff / student risk narratives the next chapter addresses the issue of problematic interpretation of on-line material. While I have considered pornography, "undesirable others" in chat rooms, hate engendering sites, websites encouraging experimentation, copyright infringement and security issues, I have said little about the problems which surround the interpretation of these concepts. It is not always obvious which material is pornographic, undesirable, hateful or dangerous. In chapter six I do not seek to provide definitions. Rather I show how some seemingly straightforward issues such as a the expulsion of a student for accessing pornography or the banning of some race hate sites were complicated by differing social interpretations.

Chapter Six

The interpretation of on-line material

Introduction

In the previous two chapters I have considered the risk narratives of staff and students. Thus I recognised that individuals were anxious about the effects of on-line pornography, the activities of "undesirable others" in chat rooms, the impact of hate engendering sites on children, the dangers offered by experimentation websites, the issue of copyright infringement and threats to network security. Yet, so far these fears have been addressed in a manner that suggests that there is no difficulty in defining what is pornographic, undesirable, hateful, dangerous to children or a legal infringement. In this chapter, I seek to illustrate that such concepts are not always easy to interpret. Indeed attempts to categorise certain on-line material may well be contested. This is not to deny that there is broad agreement in schools on what, for example constitutes hard-core pornography. Yet, there are "grey areas" where definitions become problematic. The aim of this chapter is to draw attention to some of these problematic areas.

How individuals perceive items is often a function of social construction, that is, their view is built up through social processes. Such processes may differ widely depending on the individual. This means that material and events might be interpreted differently depending upon a person's background. Interpretations of material may also differ depending on the user and the use to which such data is put (Resnick and Miller, 1996). For example while young children might in general be prohibited from accessing racist websites, older students might be actively encouraged to access such sites as part of a lesson looking at propaganda. Finally material is often interpreted with reference to a host of signs which surround it. I will argue that as the Internet potentially removes such references certain conceptual boundaries can become blurred.

In considering these issues I am not attempting to construct a framework for interpreting Internet misuse but rather seeking to illustrate how social

construction and issues of context make the labelling of certain on-line material problematic. As I am merely seeking to draw attention to general interpretative difficulties I do not provide examples from all the schools involved in my research. Rather I consider particular incidents which illustrated interpretative difficulties with regards to pornography, hate engendering sites, websites encouraging experimentation and the issue of copyright. Before considering each of these areas in turn I will first focus on social construction, the issue of context and the potential of the Internet to blur conceptual boundaries.

1. Problems of interpretation

In considering interpretative problems surrounding school internet use I shall briefly examine the concept of social construction and highlight how diverse perspectives can lead to differential labelling of the same material. In particular I will focus upon the example of the competing interpretations surrounding the *I Am a Camera* exhibition which ran throughout March 2001 at the Saatchi gallery, London. I shall then examine the importance of context and intended outcomes, noting that certain broadly unsuitable material might be reconstructed as appropriate educational data if resituated in a structured learning environment. Finally I will consider the potential of the Internet to blur conceptual boundaries.

Social construction can be described as a process whereby a phenomenon is built up through social processes rather than being a natural occurrence. From this perspective, concepts such as pornography, unsuitable material or racism should not be perceived as given "truths" but rather as categories, which are the product of wider social processes of both negotiation and enforcement. In this context, it can be argued that there are often a variety of competing interpretations.

Such differences were illustrated in the arguments surrounding the *I Am a Camera* exhibition at the Saatchi Gallery, London. Tierney Gearson, an American artist, displayed photographs at the exhibition of her naked children aged four and six. Following complaints, the Metropolitan Police Obscene Publications Unit visited the gallery and asked for the pictures to be removed and the gallery, after consulting lawyers, refused in the "name of artistic freedom"

(The Times, 13.03.01). While it was considered possible that a prosecution under the Protection of Children Act 1978 might follow, no further action was taken. The key question of whether the pictures were indecent focused in particular on an image of a naked child wearing a pig mask. While it was contested that this image and several others were intended to be provocative Gearson defended her work, saying that "only a perverted mind" could deem them obscene (The Times, 13.03.01). Although the artist attempted to invoke a discourse about the innocence and the openness of childhood, the police perceived the photographs as paedophilic material. This incident highlights the importance of differing interpretations when trying to force a meaning onto an image. Furthermore the *I Am a Camera* exhibition also highlighted the issue of context, insofar as the presentation of Gearson's photographs outside of the gallery setting might have been more likely to result in a prosecution. Relating this incident to schools, it might be seen how some members of staff could potentially interpret nude human forms in art lessons as pornographic. Even if the viewing of naked human forms in school art lessons is perceived as broadly acceptable, the same activity might be labelled as inappropriate outside of this subject area.

As Resnick and Miller (1996) note with regard to Internet use, the interpretation of appropriateness depends not only upon the supervisor but also on whom is seeking to use the material and the intended outcome. Thus, it might be acceptable for students to access racist websites but only if they are studying propaganda or other related themes. In this context, a key concern is how students use and interpret on-line material. While older students might be able to interpret race hate sites as propaganda younger students might simply take such material at face value. Thus, definitions about the appropriateness of certain material on the web may vary depending upon the age of the user. Nevertheless, it should noted that there is certain material on the web, such as illegal pornography, which will be interpreted in broadly the same manner regardless of supervisor, user and context.

The issues considered so far have been general and non-specific to the "net". However, I would argue that the Internet gives rise to its own specific interpretative problems. In particular the World Wide Web allows for the

removal and distortion of a host of referential signs that individuals use in judging the legitimacy or suitability of material. Thus images of scantily clad individuals which might be tacitly tolerated in magazine form become redefined as unsuitable or even pornographic when accessed on the school Internet. While part of the issue might well be the misuse of school resources, I would argue that the recontextualisation of such images could lead to confusion as to whether they should be relabelled as pornographic. This issue is discussed below with reference to students accessing the FHM magazine and Sun newspaper websites. User friendly website construction software means that it is not difficult to copy and recontextualise data or create new information on-line. Whereas in the media material previously required some degree of legitimacy to persuade publishers or broadcasters to make it available to a wide audience any person with on-line connection and some knowledge of website building packages can now produce information for a potential world wide audience. Thus racist organisations can produce widely available material, which mimics academic legitimacy through adopting a pseudo-authoritative presentation. This creates the problem that unless teacher's check all websites used as sources of information the quality of academic material used by students might be compromised. Thus, drawing on the work of Lawson and Comber (2000a) I would argue that the Internet potentially blurs conceptual boundaries, such as those that differentiate pornography from the aesthetic or propaganda from academic material.

Having considered interpretative differences, the issue of context and the potential of the Internet to blur conceptual boundaries I will now examine some examples of interpretative problems relating to the risks arising from school Internet use. Thus I will focus upon the issues of pornography, hate engendering sites, experimentation websites and copyright.

2 Pornography

While there were incidents in all six post-primary schools of students accessing pornography using the school Internet, in certain cases the labelling of the material as "porn" by staff was contested by students. Indeed, in some circumstances while students identified material as non-pornographic they

recognised that teacher's interpretations might differ. Furthermore, although certain sexual images were not banned in school in print form, when the same images were accessed via the school Internet they were reconstructed by staff as pornographic in nature. To illustrate these points I will consider the student discourse surrounding the accessing of an image of a scantily clad female wrestler, the disciplining of a student for visiting the Sun Page Three website and the expulsion of a student for viewing "naked female forms" on the FHM magazine website.

While students were able to identify the accessing of material of a sexual nature as misuse of the school Internet, conceptual vagueness existed as to which images were to be considered pornographic. At Dalehouse, Harry a year 10 student, was attempting to log off the Internet when background wallpaper appeared on screen showing a scantily clad woman. The picture of a female wrestler in a bikini had been downloaded from the World Wrestling Federation website. Three other year 10 boys, including Gary and Phil, quickly flocked around the computer and the following conversation ensued:

> Gary: You shouldn't be allowed on.
> Interviewer: Are you shocked?
> Gary: It's just like you get messages, it just says this may have some offensive stuff on, language and stuff. WWW.rotten.com. You can't get on it. It's got pictures like of minging things, dead people.
> Phil: [laughs] Brains in the bin.
> Interviewer: Are you not bothered a teacher will see you?
> Harry: I wasn't planning on it.
> Interviewer: Why? It's not pornographic.
> Harry: Try telling that to a teacher.

While observing Harry's attempts to remove the image from the screen, Gary and Phil didn't directly mention the bikini clad female wrestler. Instead they started to discuss websites, which contained "offensive stuff", that were filtered out. Thus Gary mentioned rotten.com a website which he claimed carried pictures of dead people and other "minging", that is disgusting, things. Phil carried on the conversation about disgusting items, by mentioning "brains in the bin", which he later explained was a description of an image accessible on the rotten.com website. In this case a picture of a scantily clad woman resulted in students

talking about websites which were filtered by the school Internet provider. Although Gary and Phil discussed examples of material on such blocked websites they did not make reference to sexual images. Nevertheless, the suitability of the "sexual image" Harry downloaded was indirectly questioned through invoking a general narrative of unsuitable images. This is not to suggest that Gary and Phil interpreted the image of the wrestler as being offensive in the same way that on-line images of brains in a bin might be. Yet, an association was obviously made. The students recognised the broader issues of censorship and suitability raised by the incident. Furthermore, while Harry implied that the image of the female wrestler was not pornographic he recognised that staff might not draw the same conclusion. Thus Harry was aware that his idea of what constituted "pornography" might not match with the interpretation of school staff.

This incident illustrated how students were aware of both censorship and differing interpretations of what constituted suitable on-line material. There was recognition that whether something was defined as pornographic depended upon the viewpoint taken.

At Greenswold the ICT manager, Robert, related how students who had been caught accessing sexual images using the school Internet had been treated "as if they [the students] had brought a pornographic magazine into school" (Robert, ICT manager, Greenswold). In cases where students at Greenswold were caught accessing commercial pornographic websites this comparison, with bringing a pornographic magazine into school, is perhaps appropriate. Yet one student was caught perusing topless female models on the Sun newspaper website. Popular British papers, such as the Sun and the Daily Star, often feature pictures of semi-naked female models. While the student was punished for accessing the "Sun page three" website using the school Internet Robert confirmed that students were not banned from bringing print copies of the actual paper into school. The print copies of papers such as the Sun carry pictures that also appear on their website. When Robert was asked if he regarded the image accessed by the student as pornographic, bearing in mind it was also printed in a daily paper, he replied the student "was on the web looking at pictures of naked women. Page

three or not ... looking at such images on the web in school we treat it all as porn" (Robert, ICT manager, Greenswold).

In this case Robert suggested that if a student uses the school Internet to view material showing naked women then the images are judged without reference to their usual off-line context.

Arguably, what was at issue here was that the student accessed this material using school equipment. Thus, it was not the image that resulted in punishment, as students were not prohibited from bringing similar images into school in print form, but rather the context in which the picture was accessed and presented. While Robert did not label the Sun or the Daily Star as pornographic publications, images of topless female models removed from these papers, placed on-line and accessed using the school Internet became reconstructed as pornography. It was not evident that students understood this distinction.

During the first term in which the Internet was installed at Hightree a year 12 student who was caught accessing what the ICT Manger Tony described as pornography was expelled. The offending picture of a "naked female form" was on the FHM website. FHM is a monthly magazine aimed at young males, which caters for the culture of "laddism". It features stories about drinking, sport, fashion, comedy and pictures of semi-naked females. Despite the sometimes sexually provocative nature of the pictures the magazine is not legally prohibited to any age group. While Tony originally described the incident at the college as an obvious example of a student accessing pornography, some of the students interpreted it differently.

Ben: Someone got thrown out [of college].
Bill: But that wasn't for games. That was...
Interviewer: Pornography?
Bill: But it wasn't though that's the thing ... what happened it was, the one [website] he was going on was the FHM Website. It's hardly porn.
Interviewer: So they caught him...
Bill: And made an example of him. A bit out of order.
Ben: It's [FHM magazine] in most shops and it's not top shelf or anything.

The above discussion with two year 13 students at Hightree highlights interpretative differences. Despite the fact that the picture was of a topless woman, the students saw this as unproblematic since the website on which it was featured was not pornographic. They supported this claim by referring to the fact that FHM was not a pornographic magazine or a "top shelf" publication. In newsagents, magazines which are pornographic, and legally prohibited to under-18's, are placed on the top shelf out of the reach of browsing children. However, in newsagents FHM magazine tends to be placed amongst other general interest men's magazines rather than on the top shelf. The students reasoned that if a print magazine was not pornographic then neither was its website. Although this assertion is clearly contestable, as it so happens in this case the pictures featured on the FHM website were comparable with those featured in the print magazine. The students seemingly interpreted the concept of pornography within a legal framework, referring to "top-shelf" publications that were prohibited to those younger than 18. In this context both the FHM magazine and website are not legally pornographic.

Tony, the ICT manager, was questioned again about this incident, after having been informed about the student's views. While maintaining that it was an example of the Internet being misused, he further explained that the issue was that a member of staff had complained:

> In this instance the issue was really a member of staff was offended by the display, in a working room, of naked female forms. It was partly that and I think it's also in no sense appropriate use ... unless you were on an art course and had to draw the female form ... It was just misusing a resource and in the second case it actually offended someone. Yeah I don't think you could do it [formal discipline for Internet misuse] on the basis of just offending someone, I think you're on dodgy ground there (Tony, ICT manager, Hightree).

While Tony remained convinced that the decision to discipline the student for accessing "pornography" was correct, he nevertheless questioned what actually constituted pornography. He highlighted the importance of someone taking offence at the offending material, while maintaining that this should not always be taken as an indication that the material was unsuitable. Furthermore, he touched upon the possible difficulty in schools of distinguishing between

pornography and art. While nudity might be seen as a legitimate area of study in art, such material might be interpreted as pornographic from other perspectives. This incident illustrated the problems surrounding the interpretation of material as pornographic. Interestingly in a wider context Tony saw this issue as an opportunity to clarify what constituted unacceptable school Internet use. When asked if FHM magazine was banned from the school, Tony replied that he doubted it. This highlights the problem of context. Students can purchase and read FHM magazine in college, yet if they access material on-line that they posses in print form then the images are reconstructed as pornographic and the activity becomes a school offence. Thus contextual issues such as how a student accesses the images, in what manner they are displayed, for what purpose the student uses the material and who, if anyone, takes offence are all key variables in whether an item is constructed as pornographic.

Tony tried to put the whole issue of interpreting on-line material as pornographic into context remarking that "[t]here's shades with everything. I really don't know where the lines should be drawn. I'm not sure that anybody does" (Tony, ICT manager, Hightree). This is not to suggest that agreement doesn't exist that certain material is pornographic, but rather to indicate that the Internet blurs the boundaries between the images of sex symbols and the sexually explicit, the aesthetic and the pornographic. For example, students in all schools were seen accessing websites dedicated to Sarah Michelle Geller, star of the television series *Buffy the Vampire Slayer*. Indeed at Eastway one sixth form male student stored over 50 pictures of *Buffy* on the school hard drive. Yet as risqué images of Sarah Michelle Geller feature on the FHM magazine website the difficulty increases in defining where the boundaries of suitability lie. This issue becomes even more problematic when pictures of a more sexual nature are fed back into fan websites accessed by children. Insofar as the Internet allows images to be viewed outside of usual contextual references, definitions may become more difficult.

Overall my concern has not been to deconstruct the issues that lie behind the interpretation of certain on-line material as pornographic but rather to illustrate how in certain circumstances particular material poses problems of interpretation.

Thus, certain images while not prohibited in school in print form become reconstituted as pornographic if accessed on the web using school resources.

3. Hate engendering sites

Two key issues emerged when considering the problems arising from the social construction of websites as "abusive". Namely, what constituted hateful on-line material and whether given a change of context, such material might be reformulated as an effective educational tool. Exploring these two questions I will draw upon discussions with Tony, the ICT manager at Hightree, Colin, a history teacher at Greenswold, and Jo, the ICT co-ordinator at Brooklands.

While there was general agreement that groups advocating ethnic violence could be interpreted as "racist", some extremist political bodies are less easy to define. Thus, ambiguity existed as to whether schools would stop students from accessing material posted on the British Nationalist Party (BNP) website. While the BNP increasingly attempt to reconstruct themselves as a mainstream political party, their policies are still widely interpreted as racist.

At Hightree the Internet Acceptable Use Policy (AUP) restricted students from accessing websites dedicated to "extreme political groups". Problematic here was the issue of what constituted "extremist". Tony, the Hightree ICT manager was asked whether he would regard the British Nationalist Party website as "extremist" and therefore restricted under school policy. He replied:

> Well that's a difficult one. They're a legitimate political party. But ... I don't know. I'm guessing we'd ban it as it probably goes against the spirit of the [AUP] agreement ... Students shouldn't be on websites that promote racism or hate. (Tony, ICT manager, Hightree).

Tony initially discussed what constituted an "extremist website" with reference to the promotion of racist or hateful attitudes. Yet it should be recognised that legitimate websites might unintentionally promote hate or racist websites might be unsuccessful in fostering malevolence. In this sense defining websites as

"extremist" solely with reference to the effects they have on the individuals accessing them might be problematic.

Despite initially arguing that websites promoting hateful attitudes should be banned Tony, the ICT manager at Hightree, later remarked that "in sociology you might want to access sites denying the Holocaust ... In that context it's a valid topic for discussion" (Tony, ICT manager, Hightree). Ultimately then Tony accepted that hateful websites might have positive educational outcomes if properly contextualised.

Colin, a history teacher at Greenswold, related how in a lesson on Nazi propaganda students had stumbled across a racist website alleging that Jewish doctors were responsible for the creation of "Gulf War Syndrome". While Colin recognised the potential of the website for misleading impressionable children, he had used it as a teaching resource as he felt it was a good example of propaganda. However, he made a distinction that while he would use such on-line material with older students he would avoid exposing younger students to it. This illustrates that whether material is constructed as suitable may well be a function of the age of the user.

In a similar vein Jo, the ICT co-ordinator at Brooklands, used an incident where a student discovered some hateful websites aimed at pop star Britney Spears to encourage students to realise that the Internet contained a vast array of different people's opinion.

> After we'd been on the Britney Spears sites last week and there were the anti [Britney sites]. Well Tammy had got onto it and then Phil started finding it and it's like 'oh on these sites you get a lot of anti-things' ... Well we discussed it and they started to realise people just have different opinions (Jo, ICT co-ordinator, Brooklands).

Thus in the proper context hate engendering sites can be used as effective learning tools. While some websites can be seen as blatantly promoting hateful attitudes, others are more borderline. Although this issue was less of a concern than pornography, in that students were not reported as intentionally accessing

"hate sites", it still posed difficult interpretative problems. Additionally even where websites were labelled as racist, recontextualising the material meant that it could provide a useful academic resource. Thus, it was accepted that if correctly presented hate engendering sites could be used to educate children about the danger of prejudice on-line. Yet, Colin felt that the ability of students to interpret hateful material as vitriolic propaganda was a function of age. Hence it might be suitable for older students to access "hate sites" for project work but it would be inappropriate for younger, less discerning, less critical students.

4. Websites encouraging experimentation

Websites featuring information on drugs or explosives can be considered as dangerous insofar as they encourage students to experiment with such items. Yet it was also recognised by Dave, the ICT manager at Dalehouse and Hannah, a geography teacher at Greenswold, that such websites might have educational uses.

While Dave, the ICT manager at Dalehouse, had expressed concern about the possible dangers of students accessing websites which encouraged experimentation with drugs, he had also noted that some "drug related" sites might be a useful learning resource. Indeed he noted that a website that a student had found focusing upon cannabis "was actually quite educational" (Dave, ICT manager, Dalehouse). Discussing the idea of educational suitability Dave referred to age of the student and legitimacy of the website. Thus talking about websites focusing on drugs, he argued:

> It depends on the student and the website. Younger students shouldn't be looking at stuff like that. Older students, well if it's relevant. But they should be valid educational sites. Not just saying 'try this' (Dave, ICT manager, Dalehouse).

While it might be easy to label some drug-related websites as legitimate, others might be more difficult, for both staff and students, to categorise.

At Greenswold Hannah, a geography and IT teacher, related how she had taught a personal and social education unit on alcoholism using the Internet to find up to date information. Although she noted, "you need to check the sites first. Some I found were just about American students drinking, fraternities and stuff" (Hannah, geography and IT teacher, Greenswold), she did remark that sites such as those of Alcoholics Anonymous provided some good links to useful educational material.

While it might be conceivable that websites providing instructions for bomb making could be used as an educational resource by AS-level chemists none of the teachers interviewed considered this issue. Of course this might reflect the tenuous relevance of bomb-making websites to the AS-level chemistry syllabus.

In conclusion, it can be seen that the issues of context and age are once more important. Not all websites containing information on drugs or explosives are potentially dangerous and some are educational. However, according to Dave and Hannah such information needs to be set in an appropriate educational framework. Dave argued that younger, more impressionable children might be negatively influenced by some experimental websites, while older ones might make effective use of such information.

5. Copyright

The issue of copyright on the Internet is an interpretative nightmare. While some images are easily recognisable as subject to copyright, the ability to alter on-line material, remove it from its initial context and resituate it makes identification of ownership difficult. If staff or students are unable to trace the source of material they copy from the Internet then it may be near impossible to ascertain whether the item is subject to copyright. This is not to deny that there is material on-line that is easily recognisable as being subject to copyright or copyleft. Material that is subject to copyleft can be legally copied and changed but not sold for profit. In considering the problematic issue of copyright infringement in the schools studied, I shall focus upon the practical interpretation of such laws in the primary schools and the formal position of the Walt Disney Company (Europe).

Even if on-line material can be identified as subject to copyright, there is currently an ambiguity as to whether companies will prosecute schools for copyright violation. Both Ella, the ICT co-ordinator at Avenue, and Jo, the ICT co-ordinator at Brooklands, stated that they believed that they would not be prosecuted for copyright violation as long as they did not make a profit from the material. Thus, both teachers were happy to cut and paste on-line images of Disney characters, which were subject to copyright, to use in teaching materials. Strictly speaking, such action is illegal.

In an attempt to understand how commercial organisations such as the Disney Company might practically apply copyright laws I sent an e-mail to their European Legal affairs office. Stating that I was posing hypothetical questions, I asked what they would do if they became aware of a school violating their copyright by using Disney images for individual pieces of work, for class worksheets and to sell for profit. Central to my e-mail was the question whether they would take legal action against a school for copyright violation. I received what appeared to be a standard response to enquiries concerning the use of Disney intellectual property. The main body of the letter stated:

> We must advise you that our established policy prevents our granting others the right to use any of our characters, or our name, in connection with activities, projects and services unconnected with us ...With regard to the specific questions you have raised, we regret that all three scenarios you have described would constitute infringement of our copyright. (Letter from Jane Gross, Manager Anti-piracy, The Walt Disney Company (Europe), 04.05.01).

While confirming that the scenarios I had outlined were all copyright violations, the question of whether the Disney Company would prosecute individual schools for such a violation went unanswered. Arguably as schools are concerned with the possibility of prosecution rather than issues of copyright this does not help to clarify the issue. If companies who are victims of copyright infringement do ever choose to prosecute schools then the issue of copyright is likely to be reconstructed with reference to legal frameworks.

Conclusion

In this chapter, I have attempted to illustrate that problems exist in determining whether on-line material is pornographic, hate engendering, dangerous or violating copyright. This is not to deny that there are cases where a wide consensus exists but rather to suggest that there are some borderline areas where interpretation may be problematic. Furthermore I argued that certain on-line material of a racist nature or encouraging dangerous experimentation could be used as educational resources following a change in context.

With regard to on-line pornography it was shown that some students have an awareness that staff interpretations of what might constitute pornography may differ from their own. Furthermore, in the case of students talking about the image of a female wrestler at Dalehouse, such on-line material was grouped together in a general narrative of items considered prohibited and filtered out by the school system. Problems also existed insofar as items that were not prohibited in schools in print form, such as The Sun page three or FHM magazine became reconstituted as "pornographic" when accessed using the school Internet. Such issues of interpretation become more problematic where images of sex symbols are risqué, and feature not only on "laddish" magazine websites but also are posted on fan sites aimed at younger children. Discussing the accessing of a "pornographic" image on the college Internet, Tony, the ICT manager at Hightree, noted that there were "shades" of interpretation with everything.

When considering hate engendering sites two main interpretative issues emerged, namely the question of what constituted hateful material and if, given a change in context, such material could be educationally beneficial. Defining material as "extremist" proved difficult. Hence Tony initially suggested that the British Nationalist Party website should be banned in college, claiming that students shouldn't access websites promoting hate. Yet legitimate websites could unintentionally promote hate, while racist websites might be ineffectual in fostering malevolence. Furthermore, it was also noted that if teachers recontextualised "hateful" on-line material then it could be used a focal point for discussions about such issues as divergent views on the web, the nature of truth

and the use of propaganda. An important consideration in the use of such material was the age of the child and how prone they were to accept such information at face value.

The same interpretative difficulties existed with drug and bomb-making websites. Indeed teachers noted that if websites on drugs were vetted and then recontextualised in an educational manner they could provide effective teaching resources. Once more, it was felt that while older students might benefit from such recontextualised information it was probably inappropriate for younger students.

Although a legal framework exists within which to clarify issues of copyright infringement, it was noted that the apparent reluctance of commercial organisations to prosecute schools led to an uncertainty as to the extent to which schools could break such laws without prosecution. Furthermore, it was argued that as material on the World Wide Web could be easily copied, altered and transferred to a different context it was sometimes difficult to establish whether a copyright existed on an item and if so, to whom it belonged.

In conclusion the purpose of this chapter has been to illustrate how concepts used by staff and students to describe on-line risks are problematic insofar as they allow for different interpretations of the same material. This is not to suggest that broad agreement does not exist on the labelling of certain Internet material but rather to illustrate how interpretative difficulties might arise. Key to understanding such difficulties are ideas of differing interpretations and context. While some of the interpretative issues considered in this chapter are broadly applicable to a range of media I argued that the Internet gave rise to some specific problems relating to the removal and distortion of referential signs. Thus I considered examples where sexual images became reconstituted as pornography when removed from their newspaper / magazine context and displayed on the web.

Having considered the problematic interpretation of certain concepts in the staff / student Internet risk narratives I will now turn my attention to assessing whether

the Internet risks described in chapters four and five are actual or perceived. In chapter seven I will assess the extent to which students are at risk on-line, while in chapter eight I will evaluate the risk to institutions posed by "dangerous students".

Part Three

Assessing staff / student risk perceptions of school Internet use

In chapter seven I assess the extent to which students are at risk from on-line pornography, undesirable others on chat-lines, websites promoting hateful attitudes and sites that encourage experimentation with drugs or explosives. In chapter eight I evaluate the risks to the institution posed by the on-line activities of the "dangerous student" with regards to school image, staff authority, copyright infringement and network security.

Chapter Seven

The "student-at-risk" on-line: Evaluating the dangers of on-line pornography, undesirable others, hate engendering sites and websites encouraging experimentation

Introduction

A consideration of staff / student risk narratives in the previous three chapters has outlined various issues relating to school Internet use. While it was broadly accepted that students might be at risk from detrimental on-line material it was also recognised that their Internet activities might be a source of danger for staff and institutions. In this chapter I concentrate on the first of these threads, the "student-at-risk", in considering the negative effects of on-line pornography, undesirable others on chat-lines, hate engendering sites and self-injury arising from experimentation websites. The threats to staff and educational institutions posed by the Internet activities of the "dangerous student" are evaluated in chapter eight.

In assessing whether on-line pornography, undesirable others, hate engendering sites and experimentation websites represented an actual danger to students I will ascertain whether the threats existed on the web, assess reported incidents in the schools during the eighteen months of fieldwork and discuss whether such events occurred in wider society. Having considered the frequency of these reported "risk" incidents I will then draw upon general arguments of the damage that such occurrences might cause. This will enable me to make judgements as to whether the risks were actual and enable me to say something, where appropriate, about the likelihood of them being realised in schools.

Having reviewed and assessed each of these risks individually, I will then draw this chapter to a conclusion. Thus, I will argue that the psychological dangers arising from students accessing on-line pornography in school were a perceived risk. I support this assertion by noting that professional concern with the psychological affects of exposure to pornographic material tends to focus on

long-term repeated exposure, something which evidence did not suggest students experienced. With regard to undesirable others, hate engendering sites and experimentation sites I note that while they offered actual risks, such dangers were statistically remote. Finding no significant risks facing on-line students, I suggest that perhaps the main dangers may be those faced by the institution. This subject is the focus of the following chapter. I will now consider in detail the risks facing students using the Internet, focusing first on the issue of on-line pornography.

1. Pornography

Fears about the effects of on-line pornography on children are widespread in British society. Simon Brooke argues that "the majority of parents are concerned that children might view sexually explicit material on-line, resulting in the corruption of innocent minds" (Telegraph, 29.06.00). The idea that the Internet is a giant library of pornography easily accessible by children is one that finds frequent expression in the media (Times, 16.11.00). While such fears might be exaggerated and sensationalised (Lawson and Comber, 2000b) they nevertheless can be seen as reflecting a basic concern. Certainly in the schools studied anxiety was expressed about the effects of pornography on students. In assessing the reality of this risk I will establish the existence of pornographic material on-line, describe incidents where students in the schools studied accessed such material and discuss such occurrences in wider society. Additionally, there is much written about the psychological impact of sexual material on children, so I will briefly consider some of these works before reaching a conclusion about the risks to students arising from on-line pornography. While some of the literature on the effects of pornography seeks to differentiate the impact on moral attitudes from general psychological effects I will make no such distinction. For the purposes of this research it is sufficient to assess whether on-line pornography has a general detrimental psychological affect.

1.1 On-line material

The pornography industry is a $56 billion global industry that has become much more mainstream in recent years (Malamuth and Impett, 2001). This is reflected in the listing of some hardcore Internet pornography companies on the Nasdaq stock exchange (Morais, 1999). Furthermore, the adult entertainment e-commerce companies have in part developed many of the technological devices that enabled the Internet to grow so quickly (Lawson and Comber, 2000b).

While some commentators, such as Morrison (Times, 16.11.00), maintain that pornography is ubiquitous on the "net" there are no accurate figures that detail the number of pornographic websites. Nevertheless a cursory analysis of the list of the 1,000 most visited websites during 2000 indicated that at least 10% were adult sex sites (Tarpley, 2001). Yet concern about on-line pornography focuses not only on the availability of such material but also its nature.

According to Akdeniz (1997), pornography on the web comes in different formats, ranging from pictures and short animated movies to sound files and stories. Furthermore it is possible to discuss sex on-line, via Internet Relay Chat Channels as well as view live sex acts (Myers, 1996). Content analysis of sexually explicit media has found that the most common images are portrayals of female nudity and men having casual sex with numerous easily accessible young women (Malamuth, 1996). On the web pornographic material ranges from soft-core depictions of nudity, through hard-core images of penetrative sex to illegal images of child pornography (Akdeniz, 1997). Concern about pornography on the Internet tends to focus in particular on deviant and illegal material (European Commission, 1996a), some of which has been labelled as "the most evil hard-core available" (Jauch, 1998: 15).

Overall, it can be seen that pornographic images exist on the Internet. Concern about such material tends to focus on its widespread availability and on the particularly deviant nature of some pornography. Having established the existence of on-line pornography I will now consider incidents in schools of students accessing such material.

1.2 Incidents in schools

In detailing incidents of students accessing on-line pornographic material I will attempt to draw a distinction between occurrences which were reported as accidental and those which were labelled by staff as intentional. Although students who intentionally accessed on-line pornography might primarily be perceived as dangerous to the school I will consider the possibility that they might also be subject to the detrimental effects of pornography. Thus in this section I will seek to describe incidents where students intentionally as well as accidentally accessed pornography. I will return to the issue of students intentionally accessing on-line pornography in the following chapter. Importantly it should be noted that, as far as I was able to ascertain, none of the reported incidents related to material that was illegal under British law.

1.2.a Primary schools

There were no reported cases of students accessing pornography, either deliberately or accidentally, at Avenue or Brooklands primary schools. Cliff the head of Brooklands attributed this to the disinclination of young children to deliberately access such material, the supervision of school Internet use and the effectiveness of the filtering software. Nevertheless, Jo the ICT co-ordinator at Brooklands did express concern that some of the websites addresses listed after the children had used the search engines contained "bad" language. Thus one year six female student at Brooklands searching for sites on Britney Spears, a teen pop icon, ended up with a list of website addresses that included "Britney Spears - pimps and hot hookers" and "Britney Spears naked". While the Internet filtering software would probably have blocked these sites if the student had clicked on the web address, the search engine nevertheless included a line of text disclosing the content of these sites.

1.2.b Secondary schools

A female student at Canalside was observed searching for information on the U.S. government. In the list of websites matching the search term was the

website address www.whitehouse.com around which her icon hovered before clicking on the website address for www.whitehouse.gov. The first of these websites, www.whitehouse.com is actually a pornographic website (see Wallace and Mangan, 1996), while the second gives access to information on the House of Representatives and the Senate. This incident can be seen as reflecting the recent trend, noted by Donnerstein and Smith (2001), of adult sites using address codes that are similar to popular Internet websites. Of course, if the school filtering software was effective then the student would have been blocked from accessing www.whitehouse.com. However, if the number of adult orientated sites using pseudo-educational web addresses grow then incidents where students accidentally access pornographic material may increase. Also at Canalside a year 10 student was banned from using the Internet for a term after he managed to access a pornographic image and set it as screen wallpaper on his terminal in an ICT classroom full of teachers learning to use the Internet. While he maintained that the ban had taught him the error of his ways he nevertheless entered the term "porn" in a search engine when I was asking him about the filtering software. Thankfully, the filtering system proved adequate and the search was blocked.

At Dalehouse there were no reported incidents of students accidentally accessing pornographic material. Yet, while I was interviewing two year 11 girls who were on the Ministry of Sound dance club website I noticed that some of the messages on the bulletin board were of a sexual nature with headings such as "FUKU". The Ministry of Sound is a moderated site that uses software that blocks offensive language. Yet material containing sexually explicit terms could still be posted on the site as long as the words were incorrectly spelt. One male student at Dalehouse intentionally accessed a pornographic website which he had constructed using his home computer and the Internet. As the website was newly constructed with an innocuous title the school software did not filter it out and he was able to access it using the school Internet. The website was discovered, blocked and the boy's parents informed.

Mary, the Head of IT at Eastway, labelled the only reported incident of a student accessing pornographic material as intentional. She described how:

> We had one student who found some kind of, it was real porn, and in an RE lesson, stupid, you know men. He puts this [pornographic image] on the background. 'Hey miss come and look at what I've done'... He was banned from the computer for a certain amount of time (Mary, IT Head, Eastway).

Mary pointed out that students might accidentally discover pornography but then intentionally use it to create mischief. In this situation she argued that she regarded the misuse of the Internet as deliberate regardless of the students' initial motives.

Kate, the ICT co-ordinator at Forestfields related how a sixth form student had searched for information for project work on the Crystal Palace in London. According to Kate:

> He was actually horrified that he typed in something that he thought was quite innocent ... he typed in Crystal Palace and it came up as an undesirable lady, shall we say, who went as Crystal Palace (Kate, ICT co-ordinator, Forestfields).

This incident illustrated that while search engines provided brief descriptions of websites allowing students to discern their content, typing in a web address takes the "surfer" directly to the website. Thus in the above example the student had typed the address www. Crystalpalace.com, directly accessing the pornographic site. At Forestfields two male students were banned from using the Internet for two weeks following incidents where they deliberately accessed pornographic images. Despite enquiries as to the nature of the material, the location of the offences or the age of the culprits staff were unwilling to discuss these occurrences. This illustrates a reluctance in some schools to discuss incidents where students intentionally access pornography.

Although Beth, a business studies teacher at Greenswold, considered the possibility of students stumbling across pornographic sites with misleading names, such as bankaccount.com, there were no reported incidents of students accidentally accessing adult material. Nevertheless, according to Robert the ICT manager there were several cases where male students were caught using the school web to look at material that was deemed pornographic. Apparently, the

offending images ranged from pictures of topless women to hardcore pornography. Indeed when the school's Internet Service Providers filtering software crashed Robert related how he had to disable the Internet for a few days as "students were typing in sex.com and up it was coming" (Robert, ICT manager, Greenswold). Robert also told of an incident were a male student had found out his friend's Internet password, logged on to the school network using it, found an unfiltered pornographic website, printed an explicit image and left it so that a teacher would find it. While the real culprit was found and punished the elaborate scheming suggests that students' motives for accessing pornography in school might be far from straightforward.

1.2.c Post-16 institution

Following the expulsion of a student from Hightree for accessing what Tony, the ICT manager, labelled as a pornographic image students reportedly became more concerned about stumbling across unsuitable material using the school Internet. Thus Tony related that after the expulsion students came knocking at his office door informing him that they had accidentally accessed unsuitable websites. Pointing out that students were highly aware that a student had been expelled for accessing pornography Tony argued that "it's likely many of these accidentally accessed websites, which students chose to report were broadly sexual in nature" (Tony, ICT manager, Hightree). The student who was expelled from the college had accessed a picture of a naked woman posted on the FHM magazine website. Following this incident no other case of a student deliberately accessing pornography using the school Internet was reported during the period of the research.

1.2.d Overview

There were no reported cases of students accessing pornographic material in primary schools. However, in post-primary schools there were occurrences in all six institutions involved in the research of students accessing on-line sexual images. Most of the incidents discussed in detail by teachers related to students deliberately seeking such images. However, with regards to the accidental

accessing of 'unsuitable' on-line material it was noted that the website addresses listed by search engines could contain sexual language, that some pornography websites masqueraded as innocuous sites and that entering such website addresses directly could take a student straight to the site. Having considered examples of students accessing pornography in school I will now consider such incidents in wider society.

1.3 Incidents in wider society

The Internet differs from traditional media such as television, radio and recorded music in that it potentially gives children and adolescents access to almost any sexual content they can find. Donnerstein and Smith (2001) stress that children often know more about the technology than adults, that home Internet systems are often unfiltered and that insofar as children have "net" access in their rooms they can access adult material in private. Such factors increase the likelihood of children viewing on-line pornography.

While little is known about how children use the Internet at home a recent Time / CNN survey of US teenagers revealed that 82 % used the Internet, 44% reported seeing X-rated on-line content and 62% said that their parents knew little or nothing about the websites they visited (Stodghill, 1998). Kahn-Egan (1998) studied the ease of accessibility of various types of sexually explicit media, including the Internet and surveyed several hundred third through eight graders about their exposure to such material. Her research showed that 48% of the sample reported visiting various Internet sites with adult content, amongst which sex websites proved the most popular. An attitude survey carried out by MORI for Readers Digest suggested that parents feared children as young as six were being exposed to pornography and violence while using the Internet (Telegraph 18.08.00). Furthermore the survey found that one in twenty children aged between seven and sixteen had seen something on the Internet which had upset or embarrassed them, a figure that rose to one in ten for fifteen to sixteen year olds (Telegraph 18.08.00).

In conclusion, it should perhaps be noted that the exposure of children to pornographic images is not a new phenomenon. In a classic US study Bryant (1985) found that the average age of first exposure to pornography was eleven for males and thirteen for females. The findings indicated that by age fifteen 92% of males and 84% of females had looked at or read *Playboy* or *Playgirl*; by age eighteen the proportion rose to 100% of males and 97% of females. Of course, what may be different about children accessing on-line pornography is the extent of exposure and the particularly disturbing nature of some of the hard-core content. It is to these considerations that we now turn in briefly reviewing the research on the psychological effects on children of exposure to pornographic material.

1.4 Research on psychological effects

Social scientific literature that addresses the impact of pornography upon children tends to concentrate upon the possible negative psychological outcomes. In particular such research focuses upon the question of whether exposure to sexually explicit images changes children's attitudes towards sex. While some commentators interpret such questions within a general psychological framework others stress the moral elements. Nevertheless, the concern remains broadly the same, focusing upon whether pornography negatively impacts on children's sexual attitudes and conduct. In contemporary research the negative impacts of pornography are broadly seen as fostering psychological unease, encouraging promiscuity, and leading to an obsession with the physical side of sex at an expense of the emotional. There is little research on children and sexual media content largely because of ethical concerns of exposing children to potentially harmful pornographic material. Furthermore, little is written about the potential of pornographic material to create a feeling of unease and disturb an individual's mental state. Donnerstein and Smith (2001) argue that this is because such effects are either seen as short term or developing into the behavioural outcomes considered by social learning, priming and cultivation theories. Drawing upon these three theories I will now consider the suggestion that exposure to sexual depictions in the mass media may have an impact on adolescents.

Social learning theory posits that mass media characters serve as potent role models to learn about sexual issues and events. Yet Berkowitz and Rogers (1986) maintain that many such media effects are transient and are subject to "time decay". Furthermore, such discussion of the role model potential is less appropriate when considering students accessing individual digitised images. Such images say less about attitudes or beliefs than television programmes or movies, where the actors are given dialogue and more substantial roles to play.

Priming provides a cognitive explanation of the short-term impacts of sexual images on youth. From this perspective it is argued that ideas brought on by viewing material in the mass media can prime other semantically related thoughts, increasing the probability that they will come to mind (Donnerstein and Smith, 2001). Yet it is far from obvious that invoking other sexual ideas will directly lead to a change in behaviour.

Finally, cultivation theory concentrates on the long-term effects that heavy viewing of sexual content may have on youngsters' beliefs about social reality. Research tends to show that heavy viewers tend to have a perception of the world that "matches" or reflects the one presented on television (Gerbner et al., 1994). Yet with regard to school Internet use it is highly unlikely that students are going to be subject to "heavy" viewing of pornographic material. Rather students are more likely to fleetingly view such images. In this sense cultivation theory is not really an appropriate perspective to apply in determining the effects of viewing pornography on the school Internet.

Overall, no firm conclusions have been reached about the general impact of pornographic material on children. While a report by the British Board of Film Classifications on the effect on children of watching porn films concluded that viewing pornography is harmful to any child, the thirty-eight psychiatrists, teachers and social workers consulted were "able to quote little evidence to support this belief" (Times, 16.11.00). Yet, the relevant question is not whether pornography affects children but rather whether a brief view of on-line sexual images in school negatively impacts on students. As much research about the effects of pornography focuses on long-term exposure I would argue that

students who briefly view pornography on the school Internet are not subject to the psychological risks considered in social learning, priming and cultivation theories.

1.5 Summary

In assessing the risk to students from on-line pornography, it is necessary to consider the number of students accessing such material and the effects of such incidents. While no students in the primary schools studied were reported as accessing pornographic material, there were occurrences in all of the other educational institutions of students viewing sexual images via the school Internet. However, none of the staff interviewed described these occurrences as commonplace, rather they were presented as rare events. Information that I gathered from observation in these schools did not challenge this assertion.

While agreement may exist that exposing children to pornography is undesirable, research tends to focus on the long-term effects. None of the staff interviewed described any of the incidents of students accessing pornography in school as being either extended or on-going. While accepting that prolonged exposure to pornography may offer an actual risk to children, I would argue that students are not exposed to such long-term hazards in schools. Occasionally accessing sexual images should not be viewed in the same light as prolonged exposure to hard-core pornography. Insofar as many students seem to actively seek such material perhaps the focus should shift from the risk to the student to the danger posed to the institution. Furthermore, as Robert, the ICT manager at Greenswold and Wilf, the IT Head at Canalside, suggested concern should be focused on children's Internet activities outside schools where they are less likely to be supervised or protected by up-to-date filtering software. Overall then I would argue that the psychological danger to students posed by accessing pornographic material on the school Internet should be labelled as a perceived risk rather than actual one. After all relatively few students were reported as accessing on-line pornography and of these none were described by staff as having undergone prolonged exposure.

2. Undesirable others

Media commentators who write about the dangers of the Internet tend to concentrate on one of two issues, the impact of Internet pornography on children and the on-line activities of paedophiles. I will now concentrate on this second issue. In assessing risks I will establish the existence of the on-line threats of undesirable others, describe incidents in school and consider whether such dangers actually exist in wider society.

2.1 On-line presence

Typed, spoken and visual communication is possible using the Internet. While many students communicate via typing on chat-lines or using e-mail, some schools also have web cameras through which they can send live video and audio footage. As in wider society, not everybody who communicates is polite or well meaning. Concern in the media and schools about undesirable others on-line tends to focus upon the activities of people who seek to physically and psychologically harm children. Some of these individuals are child sex offenders. Paedophiles use the Internet to communicate with one another, swap pictures of sex crimes and seduce children (Independent, 15.02.01) Recent police operations, such as the breaking up of Wonderland, an international web-ring of child sex offenders, starkly illustrates that paedophiles make use of the Internet. While, there is little evidence to back up the claims of Detective Chief Superintendent Keith Akerman (quoted in the Sunday Telegraph, 03.12.00) that one in five children who use computer chat rooms have been approached over the Internet by paedophiles, it is nevertheless recognised that the on-line activities of paedophiles are a cause for concern (Telegraph, 25.10.00). Central to the problem of undesirable adults communicating on-line with children is that the Internet allows them to conceal their identity, enabling them to masquerade as children.

In considering the activities of undesirable others on the 'web' I will focus upon incidents where students felt threatened, harassed or developed relationships with people met on-line.

2.2 Incidents in schools

In the schools involved in this research nothing was said about paedophiles using the Internet to swap photographs, communicate with one another, set up organisations (so-called web-rings) or recruit individuals. Rather, staff and student concern focused upon undesirable others making students feel threatened, harassed or attempting to persuade students to meet off-line. While elements of this discussion will focus upon paedophiles, and both staff and students used this term, the obvious difficulty of assessing whether people on-line have been convicted of a child sex offence means that I will often revert to the more generic term of "undesirable other".

2.2.a Primary schools

At Avenue and Brooklands primary schools no incidents were reported of students being threatened by strangers on-line. Indeed in both of these schools the use of the school Internet to access chat rooms was forbidden. The World Wrestling Federation website was banned at Avenue, because it contained a notorious chat site. Indeed the WWF chat site was recognised as a key location for adolescents seeking sexually explicit on-line communication and was labelled by Ella as a site where "dangerous sick people might lurk" (Ella, ICT co-ordinator, Avenue).

Jo, the ICT co-ordinator at Brooklands related how as part of the launch of a government Internet initiative she had taken a class along to the LEA technical centre to engage in an on-line chat session. After a while a stranger calling himself Bob illicitly gained access to the chat room and started to ask the children a variety of questions about themselves. While the session ended soon after, with the children logging off the Internet, Jo nevertheless related how she had been disturbed by the whole incident.

2.2.b Secondary schools

At Canalside a year seven girl was observed logging onto the WWF website and accessing one of the chat rooms. She related how she had a young male friend that she met on a regular basis in the chat room. No sooner had she gained access to a chat room than she was faced with a barrage of sexually explicit propositions, which scrolled down the screen. She quickly looked for her friend, was unable to find him and, ignoring offers for "cyber-sex", logged off. Worryingly some of the messages scrolling up the screen asked if anyone wanted to meet off-line. Although some of the unease might have been caused by my presence, the student appeared disturbed by the whole incident and commented that "some people are so stupid" (Amber, year 7, Canalside).

Two girls at Dalehouse related how they regularly chatted with "friends" on the Ministry of Sound website. These students, Launa and Lara, appeared to know little about their on-line "friends" beyond that they lived in London and went night clubbing regularly. Despite being only sixteen years old both girls claimed to be interested in night clubbing. They revealed that they were considering a trip down to London to meet up and go clubbing with the people they'd met on-line. While it was difficult to assess how sincere the girls were in their intention to go night clubbing in London, I believed that both their age and the financial cost would prove prohibitive. Nevertheless, it might be considered worrying that they would consider visiting people who they did not know, had only chatted to using the Internet and who lived in a distant city.

One male student at Eastway explained how, although he had used chat rooms in the past, he tended to avoid them since he had been made aware through the media of the on-line activities of paedophiles. Beyond this general fear he was unable to relate any negative experiences in chat rooms and finally admitted that despite his anxiety he still used them.

At Forestfields two girls, June and Avril, related that when they held slumber parties they tended to use their home Internet to access chat-lines. Yet they found nothing sinister about their on-line experiences rather they reported that they

found it useful to be able to talk with other people about problems in their everyday lives.

Sidney, a year 10 student at Greenswold, told how he had met his girlfriend on-line. He said that they were both interested in motor racing and had started communicating by leaving notes on the message board at the Formula One website. According to Sidney, they communicated on a regular basis for a month before deciding to meet up off-line. The girl lived about forty miles away from Sidney so he made the trip by train one weekend and they met up. They became boyfriend and girlfriend, communicated regularly using the Internet and managed to meet occasionally. While this was a relatively joyful tale about love over the "net" the risks which Sidney took are worrying. Strangely he had not thought to communicate with his future girlfriend via the telephone before making the eighty mile round trip.

2.2.c Post-16 institution

Alex, a year 12 student as Hightree, described an incident where a man with whom he had innocently started "chatting" harassed him on-line. Alex logged off the Internet but the man continued to send him messages, which were waiting for him when he logged back into the chat room. While reportedly the initial messages were little more than attempts at humorous conversation after a while the man started to send requests to meet. Alex described the situation as follows:

> I was on one [chat site] before and it was a man and he was just really bothering us. And then he found out I've got a messenger service, and he was sending messages on the computer all the time. He was on till five o'clock in the morning or something silly, sending messages to us. But he just wouldn't stop. He was asking to meet and that, I was saying no. So, I just sent a message to Yahoo telling them to stop it (Alex, year 12, Hightree).

While the initial solution to this problem was simple, it should be noted that the man could have created a new on-line identity and started sending messages to Alex once more.

2.2.d Overview

Despite staff and student concerns there were few reported incidents of students being harassed by undesirable others on-line. Indeed, in the one case where a man sent Alex, a sixth form student at Hightree, unwanted on-line messages it was a relatively easy process to e-mail Yahoo and block the sender. Overall, the examples above illustrate the potential for risk to develop. Indeed the only incidents that might raise serious concern in schools were Launa and Lara's plans to visit on-line "friends" in London and Sidney meeting up with someone who he had only previously chatted to in cyber-space. To illustrate how such incidents might have become dangerous I will now consider such occurrences in wider society.

2.3 Incidents in wider society

Recently there have been a number of cases where male adults have used the Internet to seduce young girls and persuade them to meet off-line. For example, Patrick Green, aged thirty-three, "lured" a thirteen year old girl to his home for sex after meeting her through an Internet chat room. He was jailed for five years in what was believed to be the first prosecution of its type in Britain. Green was arrested in Cumbria on his way to meet a fourteen-year-old girl who he had also befriended on the Internet while masquerading as a fifteen-year -old boy (Telegraph, 25.10.00). In another case Kenneth Lockley, aged twenty-eight, contacted a paedophile web site saying he was "desperate" for underage girls. Police in America who had set up the "fake" Internet site, passed Lockley's details to Scotland Yard's paedophile squad. Lockley was arrested and jailed for sixteen months after meeting up with undercover officers and paying £200, believing he was paying for sex with a child called Amy (Telegraph, 23.05.00). On the *Tonight with Trevor McDonald* (25.10.00) programme Carol Voderman interviewed a girl, Georgie, age thirteen, who met a sixteen year old boy in a chat room, developed a relationship, and arranged to meet up with him (Telegraph, 25.10.00). This person turned out to be a forty-seven-year-old man. Although he had been having sexualised conversations with Georgie the man was not charged due to lack of evidence. In the US Katherine Tarbox, age thirteen, developed an

on-line romance with "Mark", who she believed was twenty-four. He turned out to be Frank, forty-one, who was sentenced to eighteen months imprisonment in one of the first cases prosecuted under America's Communications Decency Act (Telegraph, 07.08.00).

The above incidents starkly illustrate that children are at risk on-line from undesirable others. While students could avoid such hazards by not meeting on-line 'friends' in the real world, it is questionable whether all children realise the risk they are taking.

2.4 Summary

The risk posed by the activities of undesirable others on-line was an actual one. In the schools studied two incidents were a potential source for concern. These were the declaration of Launa and Lara that they would travel to London to meet people they had previously only communicated with on-line and Sidney's forty mile journey to meet someone he only knew through the Internet. Furthermore in wider society children have been seduced on chat-lines and tricked into meeting up with individuals. Nevertheless while the risks are actual the likelihood of them occurring should not be exaggerated. While Robert, the ICT manager at Greenswold, had expressed fear that somewhere in Britain a student would eventually be persuaded to meet off-line and be abused he accepted that it was likely to be an extremely rare occurrence.

3. Engendering hatred

While much of the controversy surrounding the web focuses on pornography or the activities of paedophiles, on-line racism is insidious and is often targeted at children (Times Educational Supplement, 14.05.99). While the issue of racism on the Internet needs to be addressed I will expand the discussion to include other hate-related issues such as religious and sexual prejudice. Thus I will consider the existence of on-line hate material, incidents in schools where students accessed such items and the issues raised in wider society.

3.1 On-line material

The increasing utilisation of the Internet by extremists promoting hateful attitudes and harmful action against ethnic, religious and same-sex orientated groups is a cause for concern (Whine, 1997; Kallen, 1998). Since a main feature of the Internet is that it allows for the free exchange of information, such hateful material is seldom subject to supervision, regulation or sanction. The Internet allows for hate groups to present their arguments in a wide range of manners such as through building their own websites, posting notes on electronic bulletin boards, sending messages to on-line newsgroups or e-mailing others. From an educational point of view the construction by extremist groups of visually impressive websites which seek to mimic legitimate academic sites is a cause for concern. For example, the Institute for Historical Review (IHR) in California, a major promoter of Holocaust denial with pseudo-academic pretensions, has sought to use the Internet to promote its views. Such groups see the Internet as the information route for the future.

> The unique nature of the Internet makes this the information battle-ground for the future ... by contrast, television and radio require the creation of broadcast quality programmes, and reaching listeners and viewers is tied to the amount of money one can afford to spend. Books, magazines and other printed material are durable and inexpensive, but no way near so freely available, and can be confiscated by oppressive governments (Institute of Historical Review, 1995: 1).

The on-line actions of extremist groups promoting hateful attitudes and encouraging harmful activities against minorities is a cause for concern. That such groups seek to present their views on the web in a way that mimics academic legitimacy is particularly worrying for adults responsible for children on-line. It is with this issue in mind that I now consider the reported incidents of children accessing hateful websites in the schools studied.

3.2 Incidents in the schools

Concern amongst staff about websites promoting hatred related to the possibility that students would uncritically accept information from such sites. Only two

incidents were observed or reported during the research where students actually accessed material via the school Internet that promoted hateful attitudes. While a student at Brooklands primary school viewed an anti-teen celebrity site, at Greenswold students accessed a website blaming the creation of Gulf War syndrome on Jewish doctors. Each of these incidents shall be considered in turn before I turn my attention to occurrences in wider society.

A year six girl was observed at Brooklands searching for websites that were dedicated to the teen pop sensation Britney Spears. The list of sites that the search engine threw up included quite a few anti-Britney sites, espousing a hatred of the star. The girl entered the website "Britney - Hit her one more time" which opened onto a screen where a digitised hand could be moved to repeatedly hit a cartoon picture of Britney. Having briefly checked the site the student went back to the list provided by the search engine and chose a legitimate Britney fan site that included pictures and reviews. A week later Jo, the ICT co-ordinator, raised this topic relating that she had used the incident as a starting point to discuss with the students the false and hateful nature of certain on-line material.

Only one incident was reported in the schools studied where students accessed on-line material of a racist nature. At Greenswold, Colin, a history teacher related how during a lesson students had stumbled across a website that alleged that "Gulf War Syndrome" was the creation of Jewish doctors. He noted how the website "had all the tanks and people being injected, superb graphics" (Colin, history teacher, Greenswold). The discovery of the material in a lesson allowed Colin to help the students in interpreting and evaluating it. Nevertheless Colin expressed misgivings, noting that while older students were able to label such material as hateful propaganda younger students might accept it as true.

Despite the proliferation of hateful material on the World Wide Web there were few reported incidents of students accessing such items. Indeed in the above examples students accidentally stumbled across the offending websites. To put these incidents and concerns in a wider context I shall now consider what impact such material has had in society.

3.3. Incidents in wider society

Certain extremists groups such as the far right have a long history of using the Internet to promote hatred. Indeed Skelton (1994) notes that hate messages on electronic bulletin boards can be dated back to 1985. More recently the National Crime Intelligence Service submitted a report on the illegal uses of the Internet, saying, "we have identified racism as a potential problem" (quoted in Times Educational Supplement, 14.05.99). Despite the existence of websites that seek to engender hateful attitudes there is no current research assessing the impact of such material or the frequency with which children discover it on-line. Neither does it appear to be a subject of interest for the mass media, which appears seemingly fascinated by the on-line risks of pornography and paedophiles. In part this might reflect feeling that racism is a wider social problem that needs to be dealt with at a broad policy level before particular concerns such as racism on the web are addressed.

3.4 Summary

The issue of engendering hateful attitudes on the web is one that should concern educationalists and parents. Cultivating awareness, particularly amongst younger children, that on-line information might be misleading or untruthful is important. During the research two incidents were reported where students accessed "hate sites" and only one of these was a racist website. Little is known about how the existence of such information on the web influences students. Nevertheless, as the damaging nature of hateful on-line material was broadly recognised by the National Crime Intelligence Service (Times Educational Supplement, 14.05.99) and staff who discussed this issue I conclude that this risk is actual rather than perceived. However, since the reported incidence of students stumbling across such websites was low and as it was far from evident that such material was uncritically accepted, I will maintain that this risk to students in the schools studied was statistically remote.

4. Self-injury through experimentation

Only two staff expressed concern that students might physically damage themselves through either following on-line instructions advocating the use of drugs or attempting to construct explosives following a "recipe" found on the web. In assessing these risks arising from experimentation using on-line instructions I will first consider the existence of such material on the web, before describing relevant incidents in schools and wider society.

4.1 On-line material

Material which promotes experimentation with drugs, alcohol or explosives have two main elements that might cause concern for those supervising children's "surfing" activity. The first is that they might recklessly promote the abuse of certain substances, such as drugs or alcohol. Secondly certain websites encourage individuals to manufacture their own substances or devices. If students follow on-line instructions on bomb making or drug use the outcome could be physical injury or death.

Wallace and Mangan (1997) note that like obscenity and most of the other "negative material" on the Internet there is nothing new about bomb recipes. Books and magazines which describe how to make explosive devices, such as *The Anarchist's Cookbook* published by Barricade books or *Improvised explosives: How to make your own* published by Paladin, have been available for a long time in the US. Yet the construction of websites detailing "recipes" from these books have meant that they are suddenly easily accessible to children in the UK. Thus such material can be accessed from websites, such as the Candyland pages or on the alt.pyrotechnics newsgroup (Wallace and Mangan 1997: 155-6). Not only have "recipes" for creating explosives been posted on the web but also instructions of how to manufacture and prepare substances with narcotic effects. While some of these sites do little beyond promote the decriminalisation of certain drugs others contain recipes on how to manufacture narcotic substances using easily purchasable substances.

Having considered the existence of websites encouraging hazardous experimentation I will now focus on reported incidents in the schools where students stumbled across such material.

4.2 Incidents in school

There was only one incident reported in the research where a student accessed a website that could have been classified as encouraging experimentation. In this particular case the website provided information about cannabis. Having considered this incident I will then briefly reflect on the concern voiced by Wilf the IT Head at Canalside about students making bombs using web recipes.

At Dalehouse Dave the ICT manager related how he had found a student accessing a website on cannabis. He took a note of the web address and told the student to log-off. He related that later when he checked out the website for himself he found it to be informative and educational. In none of the other seven schools were any incidents reported of students accessing websites promoting experimentation with intoxicants.

While Wilf, the IT Head at Canalside, expressed concern that children might access websites which provided recipes for creating bombs he noted that no student had been caught accessing such sites using the school Internet. Indeed in all eight schools there were no reported incidents of students accessing bomb-making information on the web.

Having examined the reported incident of a student accessing what could be labelled as an experimentation website I shall now consider the frequency of such occurrences in wider society.

4.3 Incidents in wider society

The obvious risk with instructional sites such as bomb making and drug taking sites is that, in addition to promoting use of the item, any instructions regarding preparation may lead students into dangerous experimentation. Although in 1993

three teenagers in Laval, Canada were seriously injured when they built a pipe bomb following instructions on the web (Wallace & Mangan, 1997: 162) no such occurrence has been reported in the UK. However, it is worth noting that Lawson and Comber (2000b) related in their research into Internet censorship that a student in one of their fieldsite schools was suspended for accessing a bomb making website. Similarly there have been no reported incidents of students in the UK suffering long-term physical damage after following the instructions of websites encouraging the abuse of drugs. However, four year eleven pupils at a Scottish public school were rushed to hospital after creating home-made ecstasy from a recipe they found on the 'web' (BBC News On-line, 07.11.01). All four made a good recovery, but were subsequently expelled as they had violated the strict school policy on drugs (BBC News On-line, 07.11.01).

4.4 Summary

The physical dangers to students of following instructions on websites encouraging experimentation are self-evident. Yet despite this very real danger the reported frequency of students engaging in such activities in wider society is close to zero. Interestingly the subject of students making bombs to cause damage to the school or fellow pupils was never raised. With a spate of school shootings and students using home-made pipe bombs in the US the issue of bomb recipes on the web may not always remain unimportant. In conclusion, while I would label the risk posed by websites encouraging experimentation with drugs or explosives as actual, the few incidents that have occurred in wider society suggest that it is a statistically remote danger.

Conclusion

In summary I will review the risks to students from on-line pornography, undesirable others, hate engendering sites and experimentation websites. Noting that most concern about pornography related to long term exposure I argue that it is difficult to support the assertion that children are at risk from pornography accessed via the school Internet. After all it would be difficult to imagine students accessing such material in school for prolonged periods of time without

being apprehended and stopped. Thus I label the psychological risks to the student arising from accessing pornography on the school Internet as perceived. While I accept that undesirable others, hate engendering sites and experimentation sites represent actual risks I maintain that they are remote ones.

Overall, I maintain that two issues need to be considered when focusing on the subject of students and on-line pornography. Firstly it is necessary to consider the number of students exposed to such unsuitable material. While incidents were reported in all post-primary schools of students accessing pornography, staff described these occurrences as rare. Secondly the question needs to be addressed of whether students suffered negative psychological effects from accessing such material. Research into the effects of pornography tends to focus on negative outcomes arising from long-term exposure to such material. None of the reported cases in the schools studied were described as examples of prolonged exposure to on-line pornography. It is worth noting that in many of the cases described, students intentionally sought out or used pornography they had discovered on the web. While an argument can be made that students who intentionally access such material may still be at risk from their own activities I would suggest that for the school this often becomes a secondary concern to the damage that an institutions reputation might suffer. This particular point is considered in the next chapter. Furthermore, students accessing pornographic material on the school Internet may well already have seen such material outside the school. In this case any potential damage is already done prior to the student seeking such material via the school Internet. In this context I would argue that the psychological danger to students posed by accessing pornography on the school Internet should be regarded as a perceived rather than an actual risk.

Cases of adults seducing children over the Internet have been reported in the media. No such incidents were related in any of the schools studied. Indeed there was no evidence in primary schools of children even using chat-lines. At Dalehouse two girls did consider meeting up with strangers they chatted to on-line and a Greenswold student visited a girl his own age that he had previously only communicated with via the web. Neither of these cases had disastrous outcomes. Nevertheless, as incidents have occurred in wider society where

children have been sexually abused following a contact made on-line I would argue that the risk posed to students by undesirable others on the Internet is an actual one, albeit statistically remote.

While websites promoting hateful attitudes might be a cause for concern there was little evidence of students accessing them. During the whole of my fieldwork in eight educational institutions there were only two reported incidents where students accessed such websites. Importantly even in these instances the websites were subsequently used as an educational resource to promote discussion. This suggests that such websites might not necessarily negatively influence the few students who view them. Certainly there was no information in the schools studied, which suggested that such sites had negatively effected students. Nevertheless attempts by hate organisations to present their websites as legitimate educational sites is worrying, insofar as they might misinform impressionable students. Recognising the problem of hateful attitudes I would maintain that websites that seek to promote hatred offer an actual risk to students. However, as few students stumbled across such on-line material and even then staff used it for educational purposes I would argue that in schools this risk is remote.

Despite concern been expressed by staff about experimentation sites only one incident of a student accessing such a website was reported. In this case the website material which focused on cannabis was deemed to be educational by the ICT manager at the school. While I would not deny that websites that include "recipes" for drug or bomb making were an actual risk, students did not appear to be attracted to such material.

Overall I would argue that while the psychological risks to students posed by briefly accessing on-line pornography in schools were merely perceived ones, the dangers arising from undesirable others on the web, hate engendering sites and websites encouraging experimentation could be seen as actual, albeit statistically remote, risks.

Having considered the risks to students arising from the school Internet I will now turn my focus to the dangers to the educational institutions. Thus in the following chapter I consider the issues of school image, staff authority, copyright and network security.

Chapter Eight

The "dangerous student" on-line: Assessing the risks relating to school image, staff authority, copyright and network security.

Introduction

As the new information communication technology is introduced into schools it is not only students who are subject to risk but also the staff and institutions themselves. In the previous chapter I considered the risks to students posed by on-line pornography, undesirable others, hate engendering sites and experimentation websites. While I maintained that the psychological risk posed by students viewing on-line pornography on the school Internet was perceived, the remaining three risks I labelled as actual although statistically rare. In this chapter I will argue that there was a narrative thread that constructed the institution and staff as being at risk from "dangerous students". In this context the "dangerous student" can be seen as an individual who intentionally misuses the school Internet. While it would be naive to suggest that staff do not also pose a potential risk to institutions there was no evidence of this concern in the schools studied beyond the anxiety expressed by one member of staff at Canalside.

In considering the activities of "dangerous students" and the risks to staff and schools arising from Internet use I will focus on the issues of school image, staff authority, copyright and security. In considering school image I will note that while students in all the post-primary schools in the research accessed pornography and had sex chats using the school Internet no negative publicity appeared to be generated. While arguing that the threat posed by students misbehaving on the school Internet and thereby challenging staff authority was at best a muted concern I will note that it was not a new risk, but rather a continuation of existing problems of control and power. Despite observing that web-related copyright violation was rife in many schools the failure of companies to take legal action suggests that the legal risks arising from this situation were perceived rather than actual ones. Finally I acknowledge that the risks to security posed by "dangerous students" borrowing passwords and / or

"hacking" into the school network are actual. Indeed I note that as free pre-designed "hacking" software is increasingly available on the web this problem could increase.

It should be noted that while the "dangerous student" was a useful concept in considering the activities of some students in the secondary and post-16 institutions studied it was not an apt description of children's use of the "net" in primary schools. Rather in primary schools students Internet use did not pose a threat to school image, staff authority or network security.

In assessing the risks arising from school Internet use by the "dangerous student" I will now consider school image, staff authority, copyright and security in turn. In each case I will relate incidents in the fieldwork schools before considering relevant issues in wider society.

1. School image

In a competitive educational market where parents have the right to choose their children's school, image is an important asset. Schools with a good reputation for teaching, examination results, discipline and resources are likely to attract students. Hesketh and Selwyn (1999) note how the Internet can be used as an effective marketing tool, to positively reconstruct the institutional image in cyber-space. Additionally the provision of the Internet in schools is seen as a good sales point by parents and staff alike. Yet teachers in the research also expressed fears that Internet misuse by students might lead to the tarnishing of the institutional reputation. In particular, anxiety focused on the possible negative publicity arising from students using the school Internet to access on-line pornography or engage in cyber-sex. In assessing the damage to the school image arising from the on-line activities of the "dangerous student" I will consider whether incidents occurred in the schools studied and if they resulted in negative media attention. Then I will focus upon media reports of students misusing the school Internet in wider society.

1.1 Incidents in school

In attempting to assess whether student's misuse of the school Internet resulted in media attention in the schools studied, I will ascertain whether students intentionally accessed pornography, engaged in sexual on-line chat or "flamed" dignitaries. After examining each of these issues, I will relate whether any incidents resulted in newspapers stories or complaints from parents. As much of the material in this section has already been covered in chapter seven I will only briefly review it here.

1.1.a Primary schools

At Avenue and Brooklands there were no reported incidents of students accessing pornography, having sexualised on-line conversations or "flaming" dignitaries. This can largely be seen as a reflection of the effectiveness of the filtering software, a tight control on what students were allowed to do and the apparent disinterest of the young children in such activities. Rather in both schools, the Internet was used to promote a positive institutional identity. Indeed both schools had established their own websites to promote their establishment and provide an initial point of contact for other students seeking to swap ideas.

1.1.b Secondary schools

In all secondary schools there were incidents of students deliberately using the Internet to access pornographic images. A student at Canalside was banned from using the school Internet for a term after he accessed a pornographic image on the web and selected it as a background for his screen. At Dalehouse a student set up his own porn website at home, so that he could access it through the school Internet and show his friends. At Eastway in a religious studies lesson a student found an image that according to Mary the Head of IT was "real porn", and set it up as background wallpaper on the computer screen. At Forestfields two students who accessed pornographic images were banned from using the school Internet for two weeks. Finally at Greenswold several incidents occurred where students accessed on-line pornography. Indeed following the crash of the school filtering

software at Greenswold the Internet had to be disabled to stop students from visiting the sex.com website.

Thus, it can be seen in each secondary school that there were reported incidents of students deliberately using the school Internet to view pornographic images. Stories such as the student setting up his own pornographic website at home to access at school or a student accessing "real porn" in a religious lesson might be considered newsworthy. Yet, none of these incidents were reported in the media. During the period of the research none of these institutions received bad media publicity as a result of their students intentionally using the school Internet to view pornography. Furthermore, none of the schools reported any parental complaints relating to incidents where students accessed on-line pornography in school.

Despite on-line chat rooms been banned in all secondary schools, with the exception of Dalehouse, they were widely in use. Students at Canalside were seen hovering in the WWF chat rooms engaging in sexual conversations. At Dalehouse two year 11 girls were observed "flirting" in the Ministry of Sound chat room. A male student at Eastway logged into a chat room with the declared intent of enticing girls into sexual conversations. At Forestfields a sixth form student explained how he liked to go to the "Chathouse" website to have "interesting" talks with females. Finally at Greenswold it was recognised by Robert, the ICT manager that the six formers were generally engaging in cyber-sex in chat rooms.

While it might be difficult to estimate the true extent of chat-line usage or even assess the proportion of these conversations that were sexual in nature, I observed on-line sexual dialogues in all the secondary schools involved in this research. Yet the schools were not dragged into the media limelight as a result of such activities. Neither was there evidence of parents complaining about such activities.

There was no evidence of students in secondary schools "flaming" dignitaries. While at Canalside year eight boys were observed in an e-mail training session

sending messages such as "Hello daft cunt you silly biffa", "Your mothers so fat..." and "you smelly fukin (sic) rat" these were sent to fellow students in the same room. This does suggest that students were more likely to e-mail offensive messages to people they already knew. As the students receiving such messages laughed and sent similar e-mails in reply I would argue that this incident could not be described as bullying. Indeed no evidence was found during the research to suggest that students used e-mails to bully one another. At Dalehouse the ICT manager, Dave, was unconcerned about negative messages being traced back to the school as the student e-mails had the identity of the Internet Service Provider rather than the school attached.

Overall in none of the secondary schools was evidence found of students sending abusive messages to people outside the school. Rather e-mail was used to keep in contact with friends and make requests for information for project work from businesses, leisure companies and health care providers.

1.1.c Post-16 institution

At Hightree a student was expelled for accessing an image which staff described as pornographic. Yet despite this incident containing noteworthy elements, such as students contesting whether the site was pornographic, the banning of a commercial magazine website and an expulsion, the story remained unreported outside of the college.

According to Tony, the ICT manager at Hightree, it was not an unusual occurrence for students to use the school Internet to engage in sexual on-line conversations. He noted "some of the conversations were frankly obscene" (Tony, ICT manager, Hightree). Indeed some of the students interviewed for this research freely admitted to engaging in sexual on-line conversations. Despite students engaging in "cyber-sex" on the school Internet, no news stories or complaints from parents emerged.

In spite of Tony's concern that students might use the college e-mail to "flame" dignitaries no such incident was reported during the research. However, Tony did

note that when the Internet was first installed students discovered that they were able to access an internal messaging system. Abusive anonymous messages were sent using this system to fellow students and, in a few cases, teachers. This incident highlighted two tendencies. Namely that if students were going to "flame" people they would choose individuals they already knew and where possible the messages would be anonymously sent.

1.1.d Overview

In the primary schools no students were reported or observed intentionally accessing pornography, engaging in sexualised conversations on chat-lines or "flaming" dignitaries. While in the secondary and post-16 institutions students did intentionally access pornography and take part in sexualised conversations using the school Internet, such incidents were not reported in the media. Additionally during the research there were no reports of students sending offensive e-mails with the school identity attached to dignitaries. The only reported parental complaint in any of the schools related to the length of time taken to decide on a punishment for the students who had "hacked" into the Forestfields school Intranet system. Based on incidents in the schools studied it would seem that the risk of students misusing the Internet, having their activities reported in the press and tarnishing the school image was merely perceived rather than an actual one. Nevertheless for a wider assessment I shall now consider media reports in wider society of schools been "shamed" by their students' Internet use.

1.2 Incidents in wider society

Insofar as news stories about the Internet use evocative language, make gloomy predictions and exaggerate problems, the media coverage of undesirable material on-line could be labelled as sensationalistic. While the focus of media attention was often on the use of the Internet in wider society, the dangers of Internet use in schools were not ignored. Thus in the British media headlines could be found such as "Teenage students rapped over school porn network" (Sunday People, 18.10.98), "Porn risk to children" (Telegraph, 29.06.00), "Teachers fear over

Internet porn" (BBC On-Line, 09.04.98), "Net porn warning for pupils" (BBC News On-Line Education, 10.10.99) and "Safety net warning against pornography" (BBC News On-Line 11.10.99). Indeed as George Cole noted "the nightmare of every school is a front-page tabloid headline screaming that their children were found accessing hardcore pornography in the classroom" (Times Educational Supplement, 15.10.99). Despite this fear there is no apparent tendency in the media to name and shame schools in which students have used the Internet to access pornographic material.

On a national level schools where students have accessed pornographic images via the Internet have managed to avoid negative media attention. This might reflect a broad acceptance that minor incidents of Internet misuse are to be expected. Arguably if schools are going to receive bad publicity for Internet misuse then it is likely to be for incidents, which are comparable to those that that have attracted media coverage in the past. For example, Glenalmond College, near Perth received media attention following the expulsion of four year eleven pupils for making an ecstasy substitute using information found on the web (BBC News On-line, 07.11.01). In this situation I would argue that the incident was reported and the college name revealed because students at a public school "cooked up" an ecstasy substitute, ingested it and were taken to hospital. I would maintain that the accessing of on-line information about drugs added a novel element to the story but was not in itself newsworthy. Bad publicity is always a possibility when schools fail to care for students or staff act unprofessionally.

1.3 Summary

While students in the post-primary institutions in this study intentionally accessed pornography and engaged in sexualised conversations using the school Internet the schools were not subjected to media attention. Neither was there evidence of complaints from parents. Such incidents were not rare and therefore were perhaps not particularly newsworthy While in schools such offences might focus peoples attention, stimulate gossip and provide a source of titillation, they seemingly held little interest to the outside world. Arguably if a school was going to receive bad publicity for Internet misuse the incident would need to be broadly

comparable in seriousness to occurrences in schools which have attracted media attention in the past.

Post-primary students did use the school Internet to access pornography and engage in sexualised conversations. Yet despite staff fears such incidents were not reported in the press. In this context I would argue that the risk to school image posed by the "dangerous student" using the school Internet to access pornography, engage in sexual on-line chat or "flame" dignitaries was merely perceived rather than an actual one. Indeed the Internet was used as a positive marketing device in all the schools studied, with prospective students parents been shown up-to-date computer provision. Furthermore, at Avenue, Brooklands, Dalehouse, Eastway, Forestfields and Hightree school websites were developed to promote the institutions. Having considered the threat posed by the Internet to school image I shall now focus on the issue of staff authority.

2. Staff authority

The issue of Internet misuse challenging staff authority is a difficult one to assess. Certainly in the research staff expressed anxiety that students undermined their authority through accessing unsuitable material while under their supervision. Wilf the IT Head at Dalehouse declared that he saw students' denials that they had accessed chat-lines as an "affront". At Eastway Mary, the IT Head called the students who had "hacked" into the school system "tossers" who sought only to create "mischief". At Greenswold Colin a history teacher, Beth a business studies teacher and Karen a geography / PE teacher all separately expressed concern that it was difficult to control the students when using the Internet in lessons. Tony, the ICT manager at Hightree complained that students played a kind of game with him for three months continuously reinstalling a chat program that he sought to remove from the system.

Ultimately it is difficult to assess to what degree such incidents threatened staff authority and compromised the status of staff involved. Arguably the students might be concerned with entertaining themselves rather than challenging authority. If the Internet was used to challenge staff authority then I would argue

that this issue would be more usefully understood in a wider context of staff / student relations and the issue of power.

Two further points can be made when considering staff authority and the Internet. Firstly, challenges to authority can come, not just from students, but also from other staff or parents. Thus Beth, a business studies teacher at Greenswold, worried about how other staff, in particular management, might respond to incidents of Internet misuse occurring under her supervision. Secondly, the Internet can be seen as challenging the traditional role of the teacher as the "expert". Some students were more knowledgeable than staff about a key piece of educational equipment. While this in itself is not necessarily problematic some teachers may have difficulty admitting to a lack of Internet expertise.

2.1 Summary

Overall then I would suggest that if the Internet challenges staff authority it does so on the traditional grounds of discipline and knowledge. In this sense the Internet should not necessarily be seen as offering new threats to authority but rather providing a potential to expand existing ones. Yet the concern with the Internet's effect on staff authority should not be overstated. While a few teachers expressed anxiety about how the Internet challenged their authority, such concerns were generally muted. After all if teachers felt threatened by the "net" they could avoid using it in lessons. Lacking evidence to suggest that "dangerous students" misusing the Internet were challenging staff authority in a radically different way I can only conclude that such risks were actual, yet an extension of existing ones. Having briefly considered the issue of the Internet and staff authority I will now consider copyright infringement.

3. Copyright

Schools are legally accountable for material that is on their computer network that violates copyright. Thus schools may be prosecuted for student-built webpages published on the school network, which contain copyright violations. While teachers are personally legally responsible if they use material from the

web that violates copyright to construct their own teaching resources, if the resources are deemed institutional then the school is liable. Furthermore if students download pirated music files via the Internet onto the school network then again the school is liable to prosecution for breaking copyright laws. Despite this attempt to provide a simple overview of copyright laws as they apply to schools it has to be said that they are far from straightforward. Thus it is not obvious when teaching material becomes institutional rather than personal. Importantly there is little indication of the degree of copyright violation that companies are willing to tacitly tolerate in schools. Notwithstanding such difficulties I will assess the legal risks that educational institutions are exposed to from copyright violation via the Internet. Thus I will consider incidents in schools, any legal action taken and relevant issues in wider society.

3.1 Incidents in schools

In considering copyright violation in schools I will focus upon material illegally copied from the web to make resources, school webpages and students downloading pirated MP3 music files onto the school system. So-called MP3 technology provides a way of compressing the enormous music files on audio CDs to make them small enough to send across the World Wide Web.

3.1.a Primary schools

In both of the primary schools numerous copyright violations were observed. Staff and students alike were seen cutting and pasting copyright material found on the web into their own documents. At Avenue two boys were seen copying images of wrestlers from the WWF website which bore marks indicating that they were copyright protected. Ella, the ICT co-ordinator at Avenue, related how in seeking to improve a student's literacy abilities she had copied images of Disney cartoon characters into a word document so that the student could then write a story based around the images. At Brooklands a whole range of copyright material featuring images from films such as *Titanic* and cartoon characters such as *Donald Duck* were used for the students' project work and teaching resources.

Despite numerous incidents of copyright infringement, neither Avenue nor Brooklands primary schools were prosecuted during the research period. In part this might reflect that staff at both schools avoided making profit from copyright violation. Indeed when Jo, the ICT co-ordinator at Brooklands, wanted the children to make stationery to sell in a school fund raiser the students were eager to use images of the pop group Steps. However, after a discussion in which Jo explained in simple terms the copyright laws the students instead agreed to sell writing paper featuring digitised photographs of themselves.

3.1.b Secondary schools

In all five secondary schools students were observed copying on-line material into their own work, which was subject to copyright. Additionally at Forestfields and Greenswold students downloaded MP3 music files of pirated songs.

At Dalehouse students were observed illegally copying a wide range of images using the school Internet, including material from cartoons, screen-shots from computer games and fashion photographs. Similarly at Canalside students were seen illegally copying images from the web for both schoolwork and recreational purposes. One boy who wanted to design a poster for a national competition promoting cleanliness selected an image from the "net", pasted it into his document and proceeded to cut out the attached copyright symbol. At Eastway students were observed printing images downloaded via the Internet from the television series *Buffy the Vampire Slayer*. While constructing the school website, Mary the Head of IT at Eastway, thought that it would be useful if they reproduced a section of map to show the exact location of the school. However a visiting IT consultant pointed out that unless Mary received permission from the publisher of the map, in this case Her Majesty's Stationary Office, then the school would be violating copyright. At Forestfields the school Intranet carried a variety of student webpages many of which featured material subject to copyright, such as Disney artwork. Kate the ICT co-ordinator at Forestfields expressed concern about students downloading MP3 music files from the web. Many of these sound files featured pirated songs that had been copied and then posted on the web. Concern with students' downloading pirated music files was

also evident at Greenswold. Furthermore Robert, the ICT manager at Greenswold, was anxious about students copying information from the web and claiming it as their own work.

None of the secondary schools were prosecuted during the research period despite the broad range of legal infringements, such as using images subject to copyright, downloading pirated MP3 music files and plagiarising on-line work.

3.1.c Post-16 institution

At Hightree concern about copyright infringement tended to focus in particular on students downloading music files from websites that featured pirated songs. According to Tony, the ICT manager, this was a frequent occurrence in the college, which not only tied up large amounts of network memory but also left the institution open to prosecution. In addition to downloaded MP3 files students were observed copying images and written material that was legally protected. Tony considered the possibility of putting out a booklet informing students about on-line etiquette and drawing their attention to certain legal issues such as copyright. Ironically he mused that to grab students' attention he would use images from the popular adult orientated cartoon *Southpark* to illustrate the booklet. Ironically the use of such images without permission would be a violation of copyright. Despite a range of copyright infringements no legal action was taken against Hightree during the research.

3.1.d Overview

The main dangers that educational institutions faced with regards to copyright infringement was the posting of illegally copied material on their network or website and students downloading MP3 files onto the school system. Despite a range of copyright infringements in all eight schools there were no prosecutions. Furthermore, no schools in the study reported receiving official warnings, from government or commercial bodies, that they might be subjected to legal action for copyright infringement relating to the Internet. Having examined incidents in the eight schools involved in the research I will now consider whether legal

action has been taken against other educational institutions for web related copyright infringement.

3.2 Incidents in wider society

While copyright might be regarded as a key legal issue there has not yet been a case in Britain of a school being prosecuted for an Internet-related violation of this law. In part this may reflect the assertion of staff at Avenue and Brooklands primary schools that as long as educational institutions avoid making profits from copyright violation they will not be prosecuted. In personal correspondence lawyers at the Walt Disney Company (Europe) maintained that any use of its material without permission was an infringement of copyright. Yet the company ignored the question of whether they would take legal action against schools. Of course, this is a difficult issue for Disney, as prosecuting a school for copyright violation would generate an enormous amount of bad publicity. Indeed if copyright violation was widespread in Britain's 30,000 schools enforcing the law would become a logistical nightmare. Such considerations suggests that unless companies such as Disney choose to take legal action schools are unlikely to be prosecuted for images on their network that have been unlawfully copied from the web.

Illegal websites offering MP3s of current chart hits are increasingly being visited by "music-hungry" student "surfers" and any pupil downloading the latest Robbie Williams single using their classrooms Internet connection leaves the school open to prosecution under UK copyright law (Times Educational Supplement, 11.02.00). Although a UK school has yet to face prosecution over the illicit downloading of music tracks, the University of Oregon in the US was attacked by the Recording Industry Association of America (RIAA), angry that students had downloaded and distributed pirated MP3s (Times Educational Supplement, 11.02.00). Yet in this case the University was encouraged to resolve the problem itself.

The implicit threat of legal prosecution for copyright violation hangs over many schools in Britain. Yet companies, such as Disney, have shown a reluctance to

prosecute schools for what ultimately can be considered minor infringements. The issue of MP3 copyright violation is one area where commercial interests have shown themselves willing to act. Yet even with regard to MP3 files the music industry has adopted a balanced, constructive approach seeking to encourage institutions, such as the University of Oregon to resolve the problem, rather than prosecuting them without warning. Thus it might be reasonably expected that if schools were going to be prosecuted as a result of students downloading pirated music over the Internet they would be given a period of grace in which to resolve the problem internally before formal legal action was taken.

3.3 Summary

In all eight schools in this research there was evidence of copyright violation. Yet during the research no schools in Britain were prosecuted for copyright violation issues relating to the web. Arguably any company that seeks to prosecute schools for web based copyright infringement is likely to receive substantial negative publicity. In this current context the risk of legal action against schools for infringement of on-line copyright can be labelled as perceived rather than actual.

4. Security

As the use of computer networks spreads more information is stored on-line. Protecting such information from people seeking to "hack" into computer systems is an arduous never-ending task. As "hacking" becomes more sophisticated data protection systems need to constantly improve. While in the past "hackers" needed a high level of expertise to be effective the easy on-line accessibility of complex "hacking" applications with icon driven operating systems has meant that anyone with some technical knowledge can become a "hacker". Nevertheless the easiest ways to access a computer network remains gaining entry at the "human interface". That is, accessing a system through using stolen or borrowed passwords. In assessing the risks to schools arising from network security issues I will first consider incidents in the institutions studied before focusing upon such issues in wider society.

4.1 Incidents in schools

While outsiders "hacking" into computer networks might be viewed as a possible concern this was not an apparent cause of anxiety in the schools studied. All the schools had so-called firewalls, supplied by their Internet Service Providers, which ensured system integrity was not breached from the outside. However, students within institutions "hacking" into the network were seen as a serious problem. Indeed in this context, students were seen as "dangerous". In considering such incidents I shall examine system security as a general issue, students using one another's passwords and attempts to "hack" into the school network.

4.1.a Primary schools

There was no serious compromise of Internet security at either Avenue or Brooklands. However, Ella the ICT co-ordinator at Avenue related an incident where as part of a national Internet initiative some of her students were chatting on-line with other children in a specially constructed web chat room when an unauthorised adult managed to gain access. Apparently, the adult named Bob had been able to gain access to the specially designed chat site because he had entered the correct password, which happened to be "Bob". As the students were using the LEA computers at the time this story does not directly relate to the school Internet but it is nevertheless an example of how easily on-line security can be breached. At Brooklands Jo, the ICT co-ordinator, told how she had discovered a boy illicitly accessing the *Simpsons* website. Reportedly, he had watched his older sister, who was also at the school, using the Internet and had copied her password. Thus, he had gained access to a facility that was restricted to him due to his age.

Despite these incidents the integrity of the Internet networks at Avenue and Brooklands remained intact. It is perhaps unsurprising that there were no incidents where primary school students attempted to "hack" into the school network via the Intranet. Arguably younger children have neither the desire, the

ability or, heavily supervised as they are, the opportunity to "hack" into the school system.

4.1.b Secondary schools

While there were no reported incidents of students "hacking" into the school network at Canalside the IT Head, Wilf, complained that there was a tendency for students to use one another's passwords or claim that someone had used theirs to access the 'net'. This made it difficult to hold students accountable for visiting unsuitable sites. One year 10 student at Canalside declared that he knew "fifty odd" passwords belonging to others in the school. When asked how he had acquired this knowledge he replied "I just watch them. I know every letter on the keyboard. I can work out the password from where I see their fingers go" (Phil, year 10, Canalside).

At Dalehouse Dave the ICT manager labelled "hacking" into the school Internet as the most serious offence students could commit on-line. However, there were no reported incidents of students trying to "hack" into the system, although students were observed swapping passwords.

At Eastway as part of the Internet installation process an administrative Intranet was set up containing staff observation reports and internal examination questions. Mary, the head of IT, reported that she had discovered that students had used, what was referred to as a "backdoor file", to "hack" into this internal network. Drawing on information held on the administration system and gained through interviewing students, staff were able to ascertain that during a free period one Thursday morning a group of sixth form males logged onto the Internet in the IT suite with the declared aim of working on web page design. At 11.20 a.m. one of the group logged on and off several computers before choosing a visually isolated terminal at the back of the room. Using a "backdoor" program he gained access to staff files on the system, and over a period of 40 minutes copied all the files, about 390 MB worth, to an account he had created under a bogus name. The technicians discovered this security breach after the end of the school day. The following morning the Principal and IT Head interviewed the

prime suspect. According to the Head of IT, the student's key motive was to cause "disruption". Visibly upset by the incident she referred to the students who were involved as "tossers". Later that day while Mary was describing these events to me, an ICT technician noticed that the "backdoor" program had reappeared on the system and was in use. Locating the terminal and individual using the program, Mary went into the IT suite, to see what the pupil was doing. She decided not to confront the student but rather observed his activities for five minutes before returning to the technician's room. One of the technicians noted that the student had kept the backdoor file open while Mary was in the room but had managed to close it after she left. Ultimately the students involved were threatened with suspension for introducing and using the backdoor program on the school system. However, as no prompt disciplinary action was taken, much to the declared chagrin of Mary, the incidents went unpunished.

While there were no reported attempts by students to "hack" into the school network at Forestfields or Greenswold staff recognised that password swapping was rife. At Forestfields Liz the librarian declared that students swapped passwords as a sign of friendship. According to Robert, the ICT manager at Greenswold, passwords were frequently stolen. To support his claim he related an incident where a student as a prank had spied on one of his peers, copied his password, then used it to access and print material from a pornographic website.

4.1.c Post-16 institution

At Hightree Tony described several incidents where students had attempted to interfere with the school network. On one occasion, a student had attempted to access the administration account, trying over forty different passwords over the course of an hour. Jim, the Head of science, wondered if the student had seen a technician using an old password. Although the student could not be identified both Tony and Jim referred to the person as "he". In another incident at the college, a student having seen a technician change printer credits on an account, copied the programme and attempted to increase his own credits. However, as the student was not able to launch the program on the administration system the attempt failed. Finally, the discovery and misuse of an internal chat program on

the system led the technicians to delete it from the school network. However, students copied the program, hid it on the system and continued to re-install it periodically over the following three months.

4.1.d Overview

Network security was seen to be an important issue in all the schools studied. As administration is increasingly carried out on-line, material such as staff and student records, mock examination papers and financial details potentially become accessible to student "hackers". While only one serious incident occurred where students gained access to staff information there were examples of several failed attempts. Furthermore, the problem of students using one another's passwords should not be underestimated. This practice made it difficult for staff to hold students accountable for inappropriate "surfing" activities. After all, if students did not use somebody else's password when misusing the Internet they could always claim that someone had used theirs. In this context, I would argue that network security problems posed an actual risk to the schools. In examining, whether this situation is reflected in wider society I shall briefly consider the issue of "hacking" and the activities of so-called "script kiddies".

4.2 Incidents in wider society

According to Robin Cook, "hacking" can be seen as more of a threat to the UK than terrorism. He told the House of Commons that "a computer-based attack could cripple the nation more quickly than a military strike" (quoted in the Telegraph, 30.03.01). Indeed "hacking" is big business. Large corporations pay substantial sums of money to IT consultants to ensure that systems remain uncompromised. During February 2000, companies such as amazon.com, eBay, Yahoo and CNN were all victims of "hacking", costing them estimated billions of dollars (Times, 11.01.01).

Increasingly teenage e-vandals, so-called "script kiddies", use readymade "hacking" codes to cause mayhem on the "net" (Times, 11.01.01). These children are not intelligent, high-tech "hackers". Rather they use pre-designed "hacking"

software accessible on the web. If "hacking" devices are freely available on the web then students require little technical expertise to be able to create mayhem on the school network. While I was not able to ascertain whether the "backdoor" program used by student "hackers" at Eastway had been downloaded from the web, when asked Mary, the IT head, thought that this was highly likely.

4.3 Summary

School network security is a cause for staff anxiety. Confidential information such as staff reports, mock examination papers and information about pupils is increasingly stored on-line. The illegal accessing of such information could cause great embarrassment and harm the reputation of students, staff or schools. The availability of pre-designed "hacking" software on the web means that students no longer need a high level of technical knowledge to compromise network security. Indeed the stealing or borrowing of other students passwords to gain Internet access suggests that students do not even need such software to create problems. The compromise to network security can be seen as an actual risk arising from the activities of the "dangerous student". Thus, students intentionally seek to evade network surveillance or attempt to "hack" into the school system, potentially creating serious problems for both the staff and the institution.

In concluding it is worth noting that Colin, a geography teacher as Canalside was not just concerned about security issues arising from student activities on the Internet. Rather he expressed concern that technical staff had access to teachers' on-line files and school e-mail. While he maintained that he was making no allegations about the school, he did note that if technical staff wished to create mischief they could send e-mails using his address or go "surfing" on-line using his password.

Conclusion

In summary I argued that the "dangerous student" was seen as posing a risk with regards to school image, staff authority, copyright infringement and network

security. I asserted that risks relating to school image and copyright could be labelled as perceived insofar as these dangers had not been realised in wider society. While I accepted that the Internet might pose an actual risk to staff authority I noted that it should not be seen as a new problem but rather as a continuation of existing issues of power and control. Finally, I maintained that the security risk posed by "dangerous students" "hacking" into the school network was actual and potentially serious. To support these conclusions I will briefly review the arguments put forth in this chapter.

While there were no reported incidents of students "flaming" dignitaries, there were cases in all-post primary schools studied of students intentionally accessing pornographic material and having sexual on-line chats using the school Internet. Despite these incidents and fears in the national press that such occurrences might be widespread, no school was singled out for media attention. This might reflect that the accessing of on-line pornography and sexual chat-lines by students in post-primary institutions was not a rare occurrence. After all, such events occurred in all six post-primary schools in the research. In the schools studied there was also no evidence of parental complaints relating to this issue. Thus, I concluded that the threat to school image from students accessing on-line pornography, undertaking sexual conversations on chat-lines or sending offensive e-mails to dignitaries was a perceived risk. Furthermore, I pointed out that the school Internet could be used as an effective marketing device.

The issue of the "dangerous student" misusing the Internet to challenge staff authority was a difficult one to assess. This was because it was tied up with wider issues of power and control in classrooms. In the research, staff worries about this issue had been muted, possibly reflecting that it was not a new concern, but rather an extension of an existing one. I noted that the Internet might pose a challenge to the teacher's traditional role as the "expert" while maintaining that such problems could be easily avoided by teachers not using the Internet in school. Overall I maintained that the risk to staff authority posed by the Internet was actual, albeit an extension of existing issues of power and control in the classroom.

Uncertainty existed as to whether legal action would be taken for copyright infringement in schools. Certainly in all the schools studied there was evidence that staff and students broke copyright law. Additionally in Forestfields, Greenswold and Hightree there was evidence of students downloading MP3 music files onto the school system. I noted that as schools developed their own websites and allowed students to construct webpages to post on the school network copyright violations putting the school at risk of prosecution were likely to increase. Nevertheless, none of the schools studied were the subject of legal action due to copyright violation during the research period. Indeed, in the primary schools staff explained that they understood that as long as they did not profit from such violation they would not be prosecuted. In conclusion, I argued that legal action against schools arising from student copyright infringement was a perceived risk. Even when companies took action against the University of Oregon, whose students were downloading pirated music onto the college network, prosecution was not the first step, rather the institution was given the chance to resolve the problem itself.

Finally, I argued that the activities such as stealing passwords and attempting to "hack" into the school network threatened system security and could be seen as an actual risk. Indeed in seven of the eight schools students reportedly gained access to the Internet using someone else's password. At Eastway students managed to "hack" into the school system using a "backdoor" program and copy staff reports and mock examination papers. Additionally at Hightree there were several reported attempts by students to gain access to the administrator's account. With the availability of free pre-designed "hacking" software on the web this problem is likely to get worse.

It should be noted that while the concept of the "dangerous student" was useful in analysing school Internet use in secondary and post-16 institutions it was not applicable to students in the primary schools studied. Students in the primary institutions included in this research appeared to pose little risk to school image, staff authority or network security.

Overall while some of the incidents which were a source of anxiety such as students accessing pornography, sexualised chatting on-line and violating copyright occurred they did not result in the feared outcomes. With reference to staff authority the problem was seen to be a continuation of a long standing issue, namely how to control students. The "hacking" activities of the "dangerous student" in post-primary schools I labelled as an actual risk that reflected the substantial problem of Internet security in wider society.

Having described and assessed staff / student risk narratives it now becomes appropriate to consider institutional efforts to control Internet use. Thus in the following three chapters I shall examine the use of institutional rhetoric, surveillance and exclusion as instruments of school Internet control.

Part Four

Controlling school Internet use

In chapter nine I consider the attempt by schools to control Internet use through rhetoric. In chapter ten I focus upon the exclusion of both on-line material and students as a strategy of Internet control. Finally in chapter eleven I consider the concept of surveillance and detail physical / virtual observation policies adopted by the educational institutions included in this research.

While in these three chapters I make reference to the "student-at-risk" / "dangerous student" narratives I do not attempt to distinguish whether such risks are actual or merely perceived. Rather than reflecting on such assessments, which were the subject of chapters seven and eight, I instead focus on school attempts to control the Internet and alleviate risks that they believe to exist.

Chapter Nine

Institutional rhetoric: Constructing narratives of inappropriate Internet use

Introduction

Concern about risks often carries an inherent assumption that something can be done to lessen the danger. Having considered the risks which Internet use poses to students, staff and institutions I will now examine how schools respond to these dangers and seek to control on-line activity. To regard Internet control strategies solely as attempts to reduce risk is misguided. Traditionally schools are institutions of control. While institutional rhetoric, surveillance and exclusion can all be seen as attempts to avoid the perceived and actual dangers surrounding school Internet use they should also be seen in a wider context as instruments of general control.

In this chapter, I focus upon the use of institutional rhetoric as an instrument of Internet control. Institutions in the research attempted to construct discoursively what constituted inappropriate Internet use through verbal communication, Acceptable Use Policies, visual aids and third party pressure. This discourse could be seen as a direct attempt to control student Internet use.

While I note that in primary schools verbal communication was used in a constructive manner to provide a framework for judging the appropriateness of websites, in secondary and post-16 institutions it was primarily used to harangue students perceived as misusing the Internet. Acceptable Use Policies (AUPs) were not adopted by the primary schools. However, I maintain that the other schools in the research used AUPs principally to protect against the Internet activities of "dangerous students". Despite the potential benefits of visual aids, I note that only Hightree used such devices in a direct attempt to rhetorically construct inappropriate Internet use. Finally with reference to third party pressure, such as relying upon parental influence and "netiquette", I highlight how these strategies were used in schools to respond to students who had been caught misusing the Internet. In such cases, I argue that third party pressure was

used as an instrument to control the activities of the "dangerous student". In conclusion I note that while verbal communication was used constructively in primary schools to protect the "student-at-risk", in secondary and post-16 institutions such communication, AUPs, visual aids and third party pressure were used to safeguard the establishment from the "dangerous student".

In considering institutional rhetoric as an instrument of Internet control, I will now consider the use of verbal communication, AUPs, visual aids and third party pressure. Additionally with reference to AUPs and visual aids, I shall include some brief remarks relating to the effectiveness of these policies. These comments should not be seen as comprehensive attempts at assessment but rather as opportunities to include additional information that might indicate future problems of Internet control for schools.

1. Verbal communication

Instances were observed in all eight institutions where staff told students not to visit particular websites. While in the primary schools this communication tended to take the form of reasoned explanation, in the secondary and post-16 institutions students were reprimanded, frequently with no further explanation being offered. It was felt by Tony, the ICT manager at Hightree, that this reflected a view that the students in post-primary schools knew why their on-line activities were unacceptable and didn't need to be explicitly reminded what constituted acceptable Internet use. While in primary schools the focus was the "student-at-risk" from on-line activities, in post-primary institutions anxiety was centred on the Internet activities of the "dangerous student". In considering the use of verbal communication as an instrument of Internet control I will now focus upon the primary, secondary and post-16 institutions involved in this research.

1.1 Primary schools

In the two primary schools, teachers were observed responding calmly when students stumbled upon prohibited websites. Rather than berating students for

inappropriate use of the Internet, staff were seen explaining why certain websites were "unsuitable". In some cases, the students later repeated such verbal messages.

At Avenue two year six boys building their own webpage during lesson time, were "surfing" on the World Wrestling Federation Website. Due to the adult nature of many of the conversations in the chat room and pictures of scantily clad female wrestlers the WWF site was normally prohibited. Both students were aware of this and related that they had permission from their teacher to visit this site. Their teacher later remarked "I don't normally let the students go on that wrestling website, but they wanted to copy pictures of wrestlers for their website, so I explained that this was an exception" (Ella, ICT co-ordinator, Avenue). One of the boys noted "we're not normally allowed on it [the WWF website], but we're allowed to get pictures for our web page" (Gordon, year 6, Avenue). In this situation, it was evident the students understood that under normal circumstances the WWF website was prohibited.

At Brooklands, a year six student "surfing" the web during lunchtime was about to select an on-line chat site. The head, who had just entered the room, walked up behind her, laughed and said "oh no, we don't want anybody going to terrible chat rooms" (Cliff, Head, Brooklands). The student looked at the Head, and selected a Britney Spears fan website instead. Thus, a jovial reminder from the Head persuaded the student not to access a chat-line website. During one lunch break, the ICT co-ordinator Jo was seen telling students not to go to websites dedicated to the *Southpark* cartoon because they contained "bad words". The following week I observed one of the students who had been involved in the previous weeks discussion explaining to a classmate that the *Southpark* website was prohibited "because it's got swearing" (Zoe, year 6 female, Brooklands).

In Avenue and Brooklands primary schools staff explained to students not only which websites they should avoid but also why they should not access such sites. Indeed when a student at Brooklands stumbled across a hate site focusing on Britney Spears, Jo, the ICT co-ordinator, used the incident to discuss truth, differing views and how some things on the web were just people's opinions.

Overall in the primary schools verbal communication was used in a constructive manner, insofar as students were told what constituted inappropriate Internet use and given a framework for making future judgements.

1.2 Secondary schools

At Canalside the Head of IT was forceful and direct in attempting to regulate Internet use, loosing his temper on more than one occasion. During, one lunch break he was observed telling students playing games on the Internet, "no games on the computers... If you aren't doing serious work log off and go. Leave the PCs for those doing serious work" (Wilf, IT Head, Canalside). One student was too slow in hiding the game that he was playing on the web and was caught. A shouting match ensued with Wilf telling the student "I don't want to see you in here [the ICT suite] again!"(Wilf, IT Head, Canalside). Four other staff at Canalside were also observed loudly berating students in the main ICT suite for playing on-line games and not using the Internet for work.

In the Learning Resource Centre at Dalehouse staff were observed circling the room during lesson times, ensuring that students had permission to use the Internet and were on task. Yet during breaks, lunch and outside school hours staff did little to construct a framework of inappropriate Internet use through discourse. Such absence of verbal guidance was explained partly by Zed, the ICT co-ordinator who argued that "we just want students to use the Internet. We've got a filter so we're not too bothered about anything that can get through. We just want to encourage student use" (Zed, ICT co-ordinator, Dalehouse). Allowing students at Dalehouse to legitimately access on-line games and chat sites might have removed much of the need to reprimand them for activities that otherwise could have been labelled Internet misuse. Indeed the verbal haranguing that did take place tended to focus on general rules of the library, such as not wearing coats indoors or being quiet.

At Eastway, students were told by library staff to log off the Internet after they had been caught accessing chat-lines and web games. These staff were seen telling students in minimal terms that their on-line activity was inappropriate and

that they should go and do some work. The Head of IT, Mary, attempted to construct a narrative of acceptable Internet use that made direct comparisons between off-line and on-line misdemeanours. Thus when berating a student for using someone else's password and moving computer files, she informed the student that this activity was similar to going into someone else's bag and stealing their work. When students "hacked" into the school system and copied staff files she told one of the individuals involved that his activity was similar to going into the staff room and taking confidential papers. In this context, it can be seen that in verbally reprimanding students Mary attempted to draw direct comparisons between off-line activities that students accepted were wrong and comparable on-line misbehaviour. Yet, in both these cases Mary was verbally clarifying what constituted inappropriate Internet use after the students had committed offences.

A very strong narrative of what constituted appropriate Internet use existed in the Learning Resource Centre (LRC) at Forestfields. The librarian Liz was seen frequently informing students that the Internet was for "educational use only". During a ten-minute period one Thursday lunchtime she uttered this phrase twelve times. Sixth form students who supervised Internet use in the LRC after school also used this term. If Liz or the student monitors did not perceive student Internet use as "educational" then the students were told to leave the LRC. However, at no point was anyone seen explaining to the students what "educational" meant.

At Greenswold students were seen being told to log off the Internet and leave the room when their Internet activity was interpreted as inappropriate by staff. While this was done without recourse to shouting, such discourse tended to be negatively constructed. Hence, students were told to "get off" the Internet with little additional explanation. In one incident, the ICT manager Robert approached a sixth form student in the library and, remarking that the student was on a chat site, told him to log off. The student protested that he wasn't on a chat site. Robert dismissed this reply and told the student to log off anyway. Arguably what may have concerned Robert was that rather than doing schoolwork the

student was e-mailing his friends. However, Robert did not seek to explain this to the student, instead telling him to log of the Internet.

At Eastway, Greenswold and Forestfields sixth form students were given physically unobserved, but still filtered, access to the Internet. This resulted in ICT staff invoking a narrative of trust, reminding sixth form students that they enjoyed a privileged position. Unmonitored Internet access had been provided in all three institutions at the insistence of the Principals. Indeed Mary the IT Head at Eastway and Robert the ICT manager at Greenswold were both unhappy with this situation believing that the sixth form students should not be trusted. To assuage this unease Mary and Robert related how they reminded sixth form students that the current situation was one of trust and if they betrayed this trust the Internet would be disconnected from the computers in the sixth form bases. Robert remarked "I'm unhappy about it, and I tell them, 'it's a question of trust'. But they're warned. If they abuse it then I'll withdraw Internet access in those rooms" [sixth form base] (Robert, ICT manager, Greenswold). Similarly at Forestfields Kate the ICT co-ordinator talking about the Internet machines in the sixth form rooms noted "well we trust them to be mature and they know this. So they behave themselves" (Kate, ICT co-ordinator, Forestfields).

1.3 Post-16 institution

At Hightree, staff were seen calmly telling students to log off the computer when they were caught misusing the Internet. Little explanation was offered in such circumstances beyond occasional references to a shortage of Internet machines and high student demand. Tony, the ICT manager explained that staff didn't need to explain to students why their on-line activities were deemed inappropriate because they already knew. Tony reported that upon one occasion, following complaints about general behaviour around the computers, the GNVQ students had been given a loud verbal reprimand and reminded how they should behave in the main IT room. Nevertheless, the verbal staff rebukes that I observed tended to be calm and brief, with on-line students merely been told to vacate the machines when they were caught misusing the Internet.

1.4 Summary

Verbal communication about Internet use in the primary schools tended to be constructive, insofar as students were informed why certain sites were inappropriate. Indeed, following the discovery of a hate site the students at Brooklands discussed various relevant issues and were, according to the ICT co-ordinator Jo, able to construct some sort of framework by which to assess the suitability of websites. However, in the post-primary schools much of the verbal communication surrounding Internet use and risks was limited. Thus, students were observed being told to vacate the Internet with little further explanation being provided in the secondary and post-16 institutions. This might reflect the view of Tony the ICT manager at Hightree that students knew what was acceptable and so didn't need reminding. At Eastway students did receive some assistance in interpreting their "surfing" activities, but this was only after incidents had occurred and the students were been reprimanded by Mary, the IT Head. While at Forestfields students were told that they were only allowed to access educational sites on the Internet, it was not always apparent what this meant. Thus, students were able to access websites dedicated to the *Simpsons* cartoon claiming that they were building webpages, while others continued to "surf" recreationally but accessed sites that they could justifiably argue were educational in nature. Students were also seen visiting websites with moving diagrams of pumps, optical illusions and fashion photographs, all which they freely admitted bore no relation to schoolwork or any particular educational interest.

Overall, the verbal attempts to control Internet use in all eight institutions tended to focus on reinforcing what constituted inappropriate websites and on-line activity. In post-primary schools, it appeared that students were already expected to know what behaviour was acceptable and verbal communication tended to focus largely on punishing the student. While in primary schools verbal communication tended to focus upon the "student-at-risk" from the Internet in secondary and post-16 institutions there was concern with berating the "dangerous student". If students in post-primary institutions were broadly expected to know what Internet use was acceptable, such information must have

come from somewhere. In considering this factor, I shall now focus upon Internet agreements.

2. Internet agreements

In all six post-primary schools, Acceptable Use Policies (AUPs) were introduced with the intent of informing students about prohibited on-line activities and providing a formal agreement that the school could refer back to when punishing them. These single page documents listing rules for school Internet use were signed by the student, a parent or guardian and school staff. At Hightree as the students were considered adults, a parental signature was deemed unnecessary. With the exception of Eastway, all the post-primary schools drew heavily upon an exemplar AUP that had been provided by the LEA. As I shall now consider, such policies were considered by teachers to be inappropriate for primary schools.

2.1 Primary schools

In neither of the two primary schools were students asked to sign Internet Acceptable Use Policies (AUPs). Cliff, the Head of Brooklands, maintained that he didn't think such policies were appropriate at primary school level given the inability of the younger children to understand such documents, the need to avoid alarming parents and the feeling that the school did not need such measures for protection. This last point draws attention to the issue that AUPs were not only a way of informing students about acceptable Internet use but also a contract which the school could use to discipline "dangerous students". There were no plans to introduce AUPs at either Avenue or Brooklands primary schools.

2.2 Secondary schools

In all five secondary schools students were given a one page agreement outlining an Internet code of practice which both they and one of their parents had to sign. With the exception of Eastway, all these schools based this "agreement" on an exemplar that had been issued by the Local Education Authority. As the ICT co-

ordinator at Forestfields, Kate, noted the reason for adopting the document drawn up by the LEA was expediency.

> If the county solicitors have said it is ok then it seems a bit silly that this school should go against it, because then we've got to get whatever we put together to the solicitors (Kate, ICT co-ordinator, Forestfields).

Unsurprisingly then the Acceptable Use Policies which students had to sign at Canalside, Dalehouse, Forestfields and Greenswold were broadly similar in nature. The agreements were versed in general terms, avoiding, for example, reference to particular unsuitable material such as pornography, hate engendering sites or bomb-making websites. Rather students were informed that they should not access "unpleasant" or "unsuitable" materials and must report any such items that they came across. More generally, the importance of behaving in a responsible manner, using the Internet for schoolwork and reporting "unsuitable material" was emphasised. Additionally all schools highlighted their right to check students' computer files, monitor Internet activities and withdraw access to the Internet and computer systems if the students did not use them in a responsible manner. In addition Dalehouse, as the only school that officially permitted its students to access chat sites, included a sentence insisting that students "will not send personal details using the Internet unless given permission by a member of staff" (Dalehouse, Rules for the use of the Internet, 2000). Dalehouse had also experienced problems with viruses brought into school on disks, so students were informed in their Internet rules that they needed to ask permission if they were to use floppy disks brought from home. Overall the AUPs in these four schools were constructed in negative terms, insofar as they providing a list of banned activities.

Eastway issued a "home-school partnership agreement" whose content reflected the problems created by students "hacking" into the school Intranet system. While the document opened with the request that students use the Internet for "work related to school courses and activities" the focus then shifted to "using the computer system carefully", "not try[ing] to harm it in any way", and concluded that "any attempt to interfere with the computer system is a very serious offence and will be severely dealt with"(Home-School Partnership

Agreement, 2000, Eastway). Indeed, towards the end of this one page document the following passage was inserted:

> The Computer Misuse Act (1990) states that unauthorised access to computer systems is illegal. Penalties in law can be up to five years in prison and an unlimited fine for an action which is intended to cause destruction, addition to, alteration of data (for example altering another student's work), or to impair the operation of the computer (for example introducing a virus). The legal penalty for even attempting to browse through other people's work could be up to six months in prison and a £5,000 fine (Home-School Partnership Agreement, 2000, Eastway).

I asked the person who had drafted the Eastway Home-School Partnership Agreement, Mary the IT Head, if the school would be likely to invoke the Computer Misuse Act or even whether students younger than 16 could be prosecuted under this particular piece of legislation. Mary replied that "I suppose we wouldn't and probably couldn't legally use this Act against our students. Its main purpose is for effect... We just don't want a repeat of previous incidents" (Mary, IT Head, Eastway). In this case, the acceptable use document can be seen not only as an attempt to control student Internet use in school but also as an historical narrative, drawing attention to the school's previous negative experience.

Overall, these agreements, signed by students, helped to define what constituted unsuitable Internet use. The IT Head at Canalside argued that this provided students with guidelines, clarifying which Internet activities would result in punishment:

> We've introduced a sort of contract ... It states that if students are found not using the Internet as it should be used then they'll be banned from using it. It's as simple as that. If that's all down in black and white it probably makes it fairer all round and clearer to the kids (Wilf, IT Head, Canalside).

While AUPs could be seen as attempts to inform students of what constituted unacceptable school Internet use they were also seen as safeguarding the institution. Thus the ICT co-ordinator at Forestfields argued that such policies were "to safeguard the school as much as anything" (Kate, ICT co-ordinator, Forestfields). Such policies could be seen as a safeguard insofar as they stated

which activities the schools prohibited and provided a formal agreement that schools could use if they decided to punish students.

2.3 Post-16 institution

Whereas all the secondary schools insisted upon a parent's signature on the Internet agreement, it was felt that as Hightree was a post-16 institution the student's signature was sufficient. According to the ICT manager at Hightree, one student, "being awkward", refused to sign the acceptable use document and was therefore not allowed school ICT access. While the AUP at Hightree drew heavily upon the LEA exemplar, it differed in that it explicitly named certain prohibited on-line activities. Thus the agreement specifically mentioned that students should not access pornographic, chat or politically extremist websites. Nevertheless, the agreement was similar to those used by Dalehouse, Canalside, Forestfields and Greenswold in that it was negatively focused, providing a list of prohibited activities.

2.4 Summary

Neither of the primary schools introduced Acceptable Use Policies as staff felt that the children would not understand them, that they would unnecessarily worry parents and that the schools did not need them as protection. Five of the post-primary institutions introduced Acceptable Use Policies that were broadly based on the exemplar designed by the LEA. Eastway was the notable exception, where following "hacking" incidents, the AUP was focused on the issue of system security. With the exception of the Eastway AUP, all the agreements were versed in negative terms listing general forbidden activities. In this sense, the AUPs could be seen as constructing inappropriate Internet use through discourse. While the agreement at Hightree explicitly forbid students from accessing pornographic, chat and politically extremist websites, the secondary school AUPs avoided directly naming material instead using terms such as "unsuitable" and "unpleasant". While this allowed for a broader interpretation of prohibited material it also potentially created problems for students unsure as to what exactly constituted "unsuitable". Indeed the secondary school agreements could

be seen as ensuring that the schools had documentation that they could use to formally punish students and protect the institution. Arguably, if AUPs were labelled primarily as safeguards for schools then concern was not so much with the "student-at-risk" from on-line dangers but rather the institution at risk from the "dangerous student".

Out of twenty-four students who discussed signing Internet agreements only one claimed that he was able to remember the details of the document. Another student who mentioned the AUP, declared that "I didn't really read it. I just signed it. I reckon most [students] just signed it" (Larry, year 10, Eastway). Even where students did remember the details of these agreements it was quite possible that as Bill, a year 13 student at Hightree noted "it just got ignored" (Bill, year 13, Hightree). While I do not seek to offer an assessment of the effectiveness of AUPs, such observations provide a tentative indication of possible problems in using such rhetorical devices as instruments of control. Having considered the role of Acceptable Use Policies in rhetorically controlling student Internet use I will now focus on visual aids.

3. Visual aids

In schools there is a history of visual aids, such as signs, been used to remind students to be quiet, to walk in corridors or not to enter staff rooms. Such notices often give very direct messages and can be seen as attempts at controlling student behaviour. Yet, with regard to Internet use the schools involved in this research tended to make little use of such posters. During the research period none of the schools had copies of their Acceptable Use Policies on display in the IT suites. Indeed only three schools, Hightree, Eastway and Forestfields made use of posters to remind students how they should behave in the IT rooms.

Nevertheless, the importance of posters as rhetorical control devices was arguably recognised in the government's *Superhighway Safety Pack* (DfEE, 1999). Included in this pack was a poster featuring a Disney character called Doug, who hinted that students could enjoy "safe surfing" by maintaining on-line anonymity, avoiding meetings with people they've chatted to on the web, and

deleting mail from people they don't know. These hints were largely presented in negative language, telling students not to do particular things. Indeed only one of the five hints on the poster was versed in positive terms, encouraging children to express themselves using so-called emoticons (punctuation symbols typed to look like facial expressions). Despite the pack being freely available, this poster was not seen displayed in any of the eight institutions involved in this research.

In considering the general lack of use of visual aids to construct appropriate Internet use in the schools studied, I will focus on the primary, secondary and post-16 institutions in turn. Reflecting on the somewhat limited use of posters relating to IT use in Eastway, Forestfields and Hightree I will note that signs which did exist tended to be negatively versed, listing banned activities.

3.1 Primary schools

While the classrooms in which Internet machines were placed at Avenue and Brooklands were brightly decorated with an array of students' work and posters, there were no displays that directly related to acceptable Internet use. Despite the free availability of the Disney "safe surfing" poster it was not in evidence in either of these schools. Cliff, the head of Brooklands, had noted that lists were not particularly effective in teaching young children acceptable Internet use. In this light it could also be argued that posters featuring lists of Internet "do's and don'ts" might be ineffectual in informing the younger primary school children about Internet use and on-line risks. However, none of the staff in the primary schools gave any explicit explanation as to why visual aids, such as posters, were not used to reinforce ideas of acceptable school Internet use.

3.2 Secondary schools

There was little evidence in the secondary schools of attempts to define through the utilisation of visual aids what constituted acceptable Internet use. Thus in Canalside, Dalehouse and Greenswold there was no evidence of posters relating to Internet use. While posters were in evidence in Eastway and Forestfields these tended to address general issues of computer use.

At the start of my research period at Eastway a sign was attached to the single Internet machine, which read "Please send all e-mails off-line... Sending messages and using chat-lines is a waste of Internet time (10 hours a week) which is more effectively used in research". At this time the school only had ten hours free Internet access a week. While the message was generally concerned with the efficient use of limited resources, it significantly labelled e-mails and chat-lines as a waste of Internet time. Following the introduction of more widely available Internet access at Eastway no signs warning against misuse or rebuking students for accessing chat-lines were in evidence. However, a sign posted by the management briefly appeared outside the staff room at Eastway reminding teachers that they were in school to work not socialise, and that the staff room was a place of work not a café. This clearly showed an appreciation for the control potential of signs. Yet, as the research period ended at Eastway, no signs informing students about acceptable Internet use were in evidence.

While an array of signs at Forestfields advised students about general conduct and computer use in the library, these did not touch upon the issue of appropriate Internet use. Rather the posters reminded students to book computers, informed them that they could not use the printer outside the school day and asked them not to use the library socially.

During the research none of the secondary schools attached copies of their Acceptable Use Policies to walls close to Internet machines. Mary the IT Head at Eastway was asked why she did not make use of posters to remind students about acceptable Internet use, she replied "a lot of the students don't pay attention to the home / school [AUP] agreements... I don't think posters would have any effect on them" (Mary, IT Head, Eastway).

3.3 Post-16 institution

At Hightree posters were placed in the IT rooms informing students which on-line activities were deemed inappropriate. Numerous copies of a poster were pinned around the IT suites and library reminding students that "you must not use chat-lines or play games on the Internet". There were no copies of the college

AUP posted in the IT suites. Yet, insofar as chat-lines and games had been highlighted as problematic areas for Internet control, the posters can be seen as addressing the key day-to-day concerns. Although Tony, the ICT manager at Hightree, had mentioned the possibility of putting messages on-screen to advertise new services, software programs or current system difficulties he had not considered posting on-screen messages underlining what constituted Internet misuse.

3.4 Summary

Overall, only Hightree sought to make effective use of posters to remind students what activities were prohibited on the Internet. In this case, students were discouraged from using chat-lines or playing games on the web by coloured posters dotted around the IT rooms. While at Eastway and Forestfields posters were in evidence in the IT areas, these soon disappeared at Eastway when the school got wider Internet access and did not specifically relate to the Internet at Forestfields. Nevertheless, it should be noted that all posters tended to use negative language, merely outlining activities that were prohibited. None of the schools used their internal networks to place messages about acceptable on-line use on computer screens as background "wallpaper".

While visual aids could be seen as a potential Internet control tool their lack of use in the schools studied might have indicated that they were seen as relatively ineffective devices. Indeed, during an interview with Ben and Bill, two year thirteen students at Hightree, the question was asked how they knew what constituted appropriate school Internet use. While Ben laughed and read out a notice on the wall "you must not use chat-lines or play games on the Internet as it says on the wall" (Ben, year 13, Hightree) Bill noted that "well we just don't pay attention to it. It's only a notice, after all ... I even forget they're there" (Bill, year 13, Hightree). This discussion indicates that students may disregard the requests made on posters and that over time may even forget that such notices exist.

Having considered the possible rhetorical use of visual aids, I shall now focus on the influence of third parties in attempts to control Internet use.

4. Third party pressure

While staff attempted to control school Internet use through verbal communication, AUPs and, to a lesser extent, visual aids, some related how they also relied on third parties to re-inforce ideas of acceptable Internet use. In particular, staff involved parents in reprimanding students for inappropriate on-line activities as well as relying on moderated chat-lines to police on-line behaviour.

4.1 Primary schools

In both Avenue and Brooklands, there were no examples of incidents giving rise to third party pressure. This can be seen largely as a reflection of the tight control of school Internet use and the banning of chat rooms. While a situation could be imagined where students intentionally misused the Internet and parents were called into school, this did not occur in either school during the research.

4.2 Secondary schools

At Dalehouse, Greenswold and Forestfields secondary schools incidents were reported which could be broadly labelled as resulting in third party pressure.

Following an incident at Dalehouse where a student set up his own pornographic website at home so that his friends could access it from school, the site was blocked and his parents were informed of the occurrence. According to Dave, the ICT manager at Dalehouse the parents had been told "partly so that they can punish him... but also so they can make sure he doesn't do it again" (Dave, ICT manager, Dalehouse). As the offending pornographic website had been set up at home the school had to rely upon the parents' support to avoid a repeat of the incident.

Also at Dalehouse Dave, the ICT manager, related how he wasn't particularly bothered about the perceived dangers of chat-lines as the ones which got through the filtering software were "generally safe" and often moderated. He expanded

upon this point remarking that "moderated chat-lines are safe for the students. [Laughing] Actually if anything the moderated chat-lines probably encourage our students to behave" (Dave, ICT manager, Dalehouse). Two year eleven pupils at Dalehouse, Launa and Lara related how the Ministry of Sound chat room that they frequently visited was moderated. Abusive words were automatically changed into inoffensive language, as Lara observed "they change the words. My mate wrote one and instead of swearing, it said fudge you. It's so daft." (Lara, year 11, Dalehouse). Furthermore "flaming", that is typing offensive messages, was seen as unacceptable. Launa noted that "we're not allowed to harass people or the Ministry of Sound take you off the computer" (Launa, year 11, Dalehouse). In such circumstances, it can be seen that students are subject to on-line rules and norms created by third parties. The breaking of such on-line etiquette (sometimes called "netiquette") can result in the offender being ignored, berated by other users or possibly ejected from the website. Students accessing moderated chat-lines may be subjected to such third party pressure if they breach "netiquette".

The ICT manager at Greenswold related that the parents of one student caught accessing pornography on the Internet had been invited into the school and shown the material their son had downloaded using the school system. He remarked that this had a particular effect on the mother who he believed would convince the student not to undertake such an activity again.

At Eastway parents were informed of their children's attempts to "hack" into the school Intranet. Yet it is not obvious whether this was an example of the school seeking to apply third party pressure to ensure that the incident was not repeated. Indeed the parents subsequently complained that the school management was taking a long time in deciding to discipline the students. Following these complaints the school decided not to punish the students responsible. This illustrated how third party pressure can sometimes work against educational institutions.

4.3 Post-16 institution

At Hightree, Tony the ICT manager was aware of the rules governing on-line behaviour. He was particularly concerned that students did not know so-called "netiquette" and might therefore unintentionally cause offence to others. Tony considered printing a booklet giving students a rough guide to "netiquette". Arguably, in this case Tony was seeking to reinforce the effect of on-line third party pressure while also highlighting the college policy on Internet use. However, by the end of the research period the college had not issued a student guide to "netiquette".

4.4 Summary

Overall, there was little evident use of third party pressure in the attempt to rhetorically control school Internet use. The exceptions were at Dalehouse and Greenswold where parents were called into school after students accessed pornographic material. In these particular cases the ICT managers explicitly stated that the reason parents were involved was to persuade students not to engage in such activities again. At Eastway the delay in disciplining student "hackers" and subsequent parental pressure resulted in the offence going unpunished. However, it can be argued that when parents are drawn into incidents by schools there is always an element of the school attempting to invoke third party pressure to control the student.

Any student who interacts with others on-line is potentially subjected to "netiquette". The values inherent in "netiquette" can be seen as a reflection of wider social norms. However, the anonymity offered by most on-line experiences means that if students are expelled from a moderated chat site then rather than bow to third party pressure they can simply create a new on-line persona and continue acting as they wish.

Overall, involving parents and invoking "netiquette" can both be seen as examples of third party pressure concerned with controlling the activity of the "dangerous student". In the examples discussed above, no mention was made of

the student being at risk, rather the concern was to protect the institutions. Thus at Dalehouse, Greenswold and possibly at Eastway parents were involved in the discourse in an attempt to ensure that the schools were safe from a reoccurrence of these incidents. It can be noted that attempts at rhetorical control through third party pressure tended to focus on inappropriate Internet use. Thus, parents were only explicitly involved in influencing student Internet use when an offence had been committed. Although parents of students at the secondary schools included in the research were required to sign Acceptable Use Policies no evidence suggested that this led to them becoming actively involved in influencing how their child used the school Internet.

Conclusion

Verbal communication, AUPs, visual aids and third party pressure were variously used in the schools studied to control student Internet use. Staff in primary schools used verbal communication constructively to providing a framework for students to discern whether websites were unsuitable. The rhetorical approach adopted by staff at Avenue and Brooklands suggested that they perceived the students as being at risk. In the post-primary schools verbal communication, AUPs, visual aids and third party pressure were used in a way which suggested staff were concerned with the "dangerous student" and the damaging effect which inappropriate on-line activities might have on the school.

Verbal communication was used as a rhetorical control device in all the schools studied. In the primary institutions staff were observed explaining to students not only what websites were prohibited but also why they should not access them. Thus, students were provided with frames of reference that they could call upon to avoid on-line risks. However, in the post-primary institutions staff were seen reprimanding students for inappropriate Internet use with little further explanation. This might have reflected the staff assertion that students in the secondary and post-16 establishments understood which Internet activities were deemed inappropriate. If staff assumed that students already understood which on-line activities were inappropriate, then arguably the main purpose in

reprimanding a student would be to discourage them from such activities. In this scenario the student is not seen primarily as being at risk but rather as dangerous.

Staff labelled Acceptable Use Policies as inappropriate for primary schools. Nevertheless, all the secondary and post-16 institutions made use of such agreements. While they informed students, largely in general negative terms, what constituted inappropriate Internet use, they also provided a formal document to which schools could refer when punishing students. Insofar as Acceptable Use Policies were seen primarily as an instrument to protect the schools they can be seen as a response to the activities of the "dangerous students".

Visual aids, such as posters, were not widely used in the schools studied. Indeed only Hightree made use of such devices in an attempt to reinforce what constituted inappropriate Internet use. While Eastway and Forestfields had posters in IT rooms these did not explicitly address the issue of widespread Internet use in school. In general the posters used tended to be negatively worded, listing forbidden activities. Overall it can be surmised that the posters at Hightree were put up primarily to protect the institution from "dangerous students".

Third party pressure was not widely used in the schools as a rhetorical control device. Nevertheless, decisions were made to involve parents after students had abused the school technical resources at Dalehouse, Greenswold and Forestfields. While on-line students were subject to "netiquette" it was only when they transgressed the social norms that they were likely to be reminded of what constituted appropriate behaviour. In both these cases, third party pressure can be seen as a rhetorical attempt to control the "dangerous student" following a transgression.

Overall, the rhetorical devices of verbal communication, AUPs, visual aids and third party pressure can be seen primarily as instruments through which post-primary schools sought to protect themselves from "dangerous students"

intentionally misusing the Internet. In contrast, verbal communication in primary schools was used to warn the "student-at-risk" about on-line dangers.

Having considered attempts to control student Internet use through institutional rhetoric I will now focus upon the issue of exclusion. Thus I will examine the use of filtering software and the range of both formal and informal exclusion policies adopted in an attempt to control students' on-line activities.

Chapter Ten

Exclusion as a form of Internet control

Introduction

In the previous chapter, I considered institutional rhetoric as an instrument of Internet control. Such policies were not always effective insofar as they did nothing to protect students from accidentally accessing unsuitable Internet material and could often be ignored. In this chapter I consider filtering software and excluding students as forms of Internet control.

With regard to the Internet, exclusion was used to alleviate risks in the schools studied in two main ways. Firstly, dangerous material and individuals outside the school were excluded. Secondly students who intentionally misused the Internet were excluded from on-line activity, ICT rooms or even ultimately the school. While the first of these activities seeks to ensure that risks which are external to the school remain outside of it, the second attempts to resituate an internal risk outside the area in which it poses a threat to the institution. In exploring these issues I will focus upon the software and general policies adopted by schools to exclude unsuitable on-line material and students.

In considering the exclusion of unsuitable on-line material, I first seek to describe the software applications available. Thus, I consider the use of website "lists", keyword matching, graphic content management programs and keyword monitoring packages. Having described these applications, I then identify which ones were used by the primary, secondary and post-16 institutions involved in this research. While I argue that the primary schools used filtering software to protect students seen to be at risk, I note that in the secondary schools such products were also used to safeguard the institution against intentional Internet misuse by "dangerous students". Indeed, I suggest that in the post-16 institution concern with the "dangerous student" was the prime motivation for using filtering software.

Having considered the exclusion of unsuitable on-line material from schools, I then turn my attention to the exclusion of students as a form of Internet control. Thus, I note that in primary schools concern with excluding students focused on the youngest children and can be seen as an attempt to shield students from unsuitable on-line material. In the post-primary institutions, while some policies such as the introduction of booking systems can be seen as attempts to allow wider access to the Internet, I argue that the dominant narrative was one of protecting the institution against the "dangerous student". Hence, in describing institutional attempts both to limit initial student access to the Internet and expel students, I observe that policies such as locking rooms, disabling Internet access, throwing students off the Internet, evicting them from IT rooms and expelling them from school arose in response to intentional misuse of the Internet.

Before I focus upon the exclusion of unsuitable on-line material, it should be noted that at certain junctures I raise issues regarding the effectiveness of particular "exclusion" techniques. It is not my intent to provide a comprehensive assessment of the various Internet filtering software or exclusion policies, rather I merely make observations in passing that might indicate possible problems.

In considering how schools seek to control the Internet through excluding material I will first focus upon the various filtering software available before describing the applications used by the primary, secondary and post-16 institutions involved in this research.

1. Excluding material

Schools excluded unsuitable on-line material using a variety of software applications. Several filtering programs were available to schools, utilising "lists", keyword matching, keyword monitoring and graphic content management. Additionally, the Internet Service Provider provided the schools with firewalls, that is computers "configured for security reasons to filter and control network traffic to and from the outside world" (BECTa, 1998: 60). While firewalls are intended to prevent unauthorised access to private networks and provide a security control point enabling sites to connect safely to other

networks, filtering software prohibits individuals from accessing unsuitable material via the Internet. Before describing the filtering software that the schools in this research adopted, I will briefly consider the different applications available, namely "lists", keyword matching, graphic content management and keyword monitoring programs.

Filtering software that lists websites tends to take one of three particular approaches, namely allowing sites, denying sites or using neutral labelling. Software that "allows" access to a list of vetted, permitted sites has the disadvantage that students are prohibited from undertaking general searches on the World Wide Web. The use of "deny lists" means that students can search the entire web, but are blocked from accessing certain previously identified websites. The drawback of "deny lists" is that websites need to be identified before they can be blocked, a task which considering the exponential growth of the World Wide Web is becoming increasingly difficult. In addition to "allow lists" (whitelisting) and "deny lists" (blacklisting) some service providers use a third alternative, namely "neutral labelling". This attaches a content label to a site allowing a judgement to be made without visiting the website. PICS (the Platform for Internet Content Selection) is a neutral labelling system widely used in the USA. Browsers can be configured to recognise and read PICS tags, blocking access where necessary (BECTa, 1998: 49). The Internet Watch Foundation, an organisation set up by the Internet provider associations, the Government and police, is developing a European system for visibly tagging web pages with indicators similar to film ratings. The drawback with neutral listing is that websites need to be classified before the system is effective.

A key problem with filtering systems that block websites, such as "deny lists" is the durability of networks and the possibility of circumventing blocking. The Internet developed from systems designed to survive nuclear conflict. As a result it not only has a large amount of redundancy built into the system but also interprets attempts at censorship as damage and tries to route around them. Thus a site might be blocked but students might be able to find a way around the censorship and access a link that hasn't been obstructed. Indeed Phil a year 10 student at Canalside highlighted this issue when he noted "I can get around it [the

filtering software] sometimes. I just go round try different links. Try to get round it. I've done it before" (Phil, year 10, Canalside).

Keyword matching systems block searches and websites containing previously determined words or phrases. If the filter finds any matches, it will either completely block access to the site or the offending words will be stripped from the page when it is displayed. This can mean that the user is unaware that the filter has altered the page viewed. While the list of keywords can be customised to allow some flexibility in the user's Internet access, some key words are deliberately misspelled on unsuitable websites to thwart such filters. Furthermore unlike "deny lists" keyword matching may not be able to block undesirable images if the webpage does not contain any text to trigger the filter. Problematically keyword matching software might block innocuous material because it contains a prohibited word. Thus, some systems might not allow users to search for information on Essex or breast cancer as the filter recognises only the keywords sex and breast failing to distinguish the context.

Software filters exist that focus specifically upon blocking undesirable images. "I-Gear for Education" is a content management application that block images that have large areas of flesh tone colours. However, such software blocks artwork as well as pornography. Furthermore, such packages do little to filter out pornographic images on the web, which are not in colour, or unsuitable material of a non-visual nature.

"Keyboard monitoring" products check for inappropriate input on the keyboard against a pre-set list. This application tends to be used for stopping outgoing information such as credit card numbers, addresses and telephone numbers. While this software is useful in restricting outgoing information it does nothing to block incoming material. Moreover as each piece of information to be blocked needs to be individually entered these applications are more practical for home rather than institutional use.

An additional form of on-line censorship that, while not controlled by the schools, still prohibits students from accessing certain websites is third-party on-

line security. As Akdeniz (1997) notes some adult orientated sites have a security check, such as "Adult watch", where individuals must first enter a credit card number to prove they are an adult, before being given a password that allows access to a range of pornographic sites.

Having explored the various software applications available to schools to exclude undesirable on-line material I will now consider the packages utilised by the primary, secondary and post-16 schools involved in this research. All the schools in this study had "firewalls" provided by their Internet service providers. As these "firewalls" were concerned with stopping unauthorised access from outside the school networks, rather than blocking unsuitable material I will not include them in the following analysis.

1.1 Primary schools

Both Avenue and Brooklands primary schools used filtering software that denied access to certain "unsuitable" websites and blocked sites that contained previously determined keywords. While both schools could add to the website "deny list" by simply phoning their Internet Service Provider neither reported that they had actually done so. Indeed, prohibited websites were not always added to this list. Thus, Ella the ICT co-ordinator at Avenue decided that students should not access the World Wrestling Federation website, but relied on students knowing that it was prohibited rather than adding it to the Internet "deny list". While Cliff the Head of Brooklands noted that he had briefly considered giving students access to only certain allowed sites, a so-called "walled garden", he had decided that this diminished the educational potential of the Internet.

Both the Heads of Avenue and Brooklands primary schools maintained that "deny lists" and keyword matching software were used to protect students from accidentally accessing unsuitable material on-line. Indeed when I suggested to the Head of Avenue that the applications might also protect the school from intentional misuse he asserted that "we don't really have problems with stuff like that. These are young children. We don't have the same problems as in secondary schools" (Rick, Head, Avenue). I would argue that filtering software at Avenue

and Brooklands was primarily utilised to protect "students-at-risk". Indeed, there was no suggestion from staff in either of these two schools that it might be used to protect the institution from the "dangerous student".

1.2 Secondary schools

All of the five secondary schools in the research used applications that blocked certain "undesirable" websites. John, a year 13 student at Forestfields, remarked that "most of the web addresses blocked by schools are porn... images or adult chat-lines" (John, year 13, Forestfields). According to ICT technicians some race hate sites were also blocked. Following incidents of students accessing indecent material new websites were added to these 'deny' list in all five institutions. Thus websites including pornographic material were added to the "deny list" at Dalehouse, Canalside, Eastway, Forestfields and Greenswold. For example, at Dalehouse a student's home made pornographic website was blocked, while at Forestfields Kate the ICT co-ordinator reported how a site dedicated to a porn star called Crystal Palace had been blocked. These two examples illustrate that filtering software was sometimes used to block pornographic sites which students had already accessed. Overall filtering software prohibited students from accidentally and intentionally visiting unsuitable websites. In this regard "deny lists" could be seen as offering protection both for "students-at-risk" and institutions threatened by the activities of the "dangerous student".

Yet it was not just the web addresses of pornographic sites that were added to "deny lists". At Dalehouse a drug related website was blocked, while at Eastway sites interpreted as promoting animal cruelty were added to the list. Although the Internet service providers regularly updated "deny lists", the development of new "unsuitable" websites meant that such lists were never comprehensive.

The closest any of the secondary schools came to a establishing "allowed lists" was the setting up of Intranets. At Eastway work began building an Intranet, with the declared aim of placing educational resources on it. If on-line access had been limited solely to the Intranet then this would have been a "walled garden" of sorts, with only approved internal links permitted. Yet the declared intention was

that the Intranet would supplement the more general information found on the World Wide Web. Although after several incidents of Internet misuse, Mary, the IT Head at Eastway did joke that with a good enough Intranet there would be no need for the students to have access to the Internet. Yet rather than providing a secure environment the Intranet at Eastway was a source of problems, with students "hacking" into the administration system and copying staff files.

All five secondary schools also used filtering software that blocked searches or websites containing certain keywords. For example at Dalehouse Phil a year 10 student, sought to illustrate the effectiveness of the Internet filter by entering the word "porn" into the search engine. Fortunately, the software did its job, blocking the search. Yet problematically keywords on some websites were spelt incorrectly, which meant that the sites were not filtered. A year 13 student at Forestfields illustrated this point, remarking that:

> They [the school] can filter the links. If it contains the word chat, it's filtered. Link names, just certain words. You can get round it. I mean there's one we visit the Chathouse, it hasn't got any spaces in the words. So, it gets around it easily. It's pretty simple (John, year 13, Forestfields).

According to John while searches for websites using the word chat were blocked, the phrase Chathouse was not filtered and thus he could access this chat-line.

Both Canalside and Forestfields secondary schools reported that they used a content management application called I-Gear, which "scans the image for sort of flesh tones, and shuts out images with a lot of flesh like colour" (Wilf, IT Head, Canalside). According to Wilf such software was effective in blocking much pornographic material yet ineffectual in prohibiting students access to adult orientated chat-lines.

Overall, the array of filtering software used in the secondary schools can be seen as excluding material to protect the "student-at-risk" and safeguard the institution from the on-line activities of the "dangerous student".

1.3 Post-16 institution

Hightree had an internal "deny list" which they could add websites to themselves, avoiding the need to contact their Internet Service Provider. After a student was punished for accessing "pornographic" images the FHM magazine website was blocked. However, as Tony the ICT manager at Hightree noted only websites not individual webpages could be filtered out. Indeed Tony referred to the filtering software used by the college as a "blunt instrument", which did not allow the blocking of material within websites.

The college also used keyword matching software which prohibited web searches using certain pre-selected unsuitable words. While Tony had considered using graphical content filtering software such as I-Gear, he reported that he had decided against it. Thus he argued that:

> You couldn't block sites on the basis of flesh tones, for instance, because with art students the books they've got down there [in the art room] are full of human figures. Anatomy is an important part of what they do (Tony, ICT manager, Hightree).

Tony explained that as the students were young adults he was not particularly concerned about filtering software protecting them from accidentally accessing unsuitable on-line material. Rather he felt "it's there [the filtering software] to ensure students can't wilfully seek out banned items, which they really shouldn't be viewing in college" (Tony, ICT manager, Hightree). In this sense, Tony suggested that the main purpose of the filtering software was to protect the college from "dangerous students" misusing the Internet.

1.4 Summary

All the schools in the research used "deny lists" and keyword matching software to exclude unsuitable on-line material. In addition, Canalside and Forestfields secondary schools used I-Gear software that blocked Internet images with large amounts of skin tone. Insofar as filtering software was intended to stop students from accidentally and intentionally accessing unsuitable material, concern could

be seen as focusing both upon the "student-at-risk" and the "dangerous student". However, in the post-16 institution Tony the ICT manager explained that as the students could be considered young adults he was not particularly concerned about the risk to them from accidentally accessing unsuitable material. Rather he saw the primary purpose of the filtering software as protecting the institution from intentional Internet misuse.

None of the schools made use of keyword monitoring or neutral labelling packages because of practical application problems. Entering the addresses of all students to stop them from revealing this information on chat-lines or in e-mails would be extremely labour intensive and need almost constant updating. Indeed keyword-monitoring products are aimed at the home market, where with little difficulty a parent can enter a single address, phone number or credit card number and thereby stop their child from revealing such information. While neutral labelling software could be effective, it largely depends on the existence of universal, up-to-date, easily identifiable classification systems.

In conclusion, it can be seen that the schools used a variety of filtering software to exclude undesirable on-line material. While in the primary schools such software was used solely to protect students perceived to be at risk on-line, in the secondary institutions such applications were also used to stop "dangerous students" intentionally accessing unsuitable material. Indeed, in the post-16 college Tony the ICT manager suggested that the primary reason for the use of filtering applications was to restrict the on-line activities of mischievous students.

Having focused upon the software programs used by schools to exclude material I will now examine the other main way in which schools used exclusion as a means of control. Thus, I will consider how schools controlled Internet use by excluding students.

2. Excluding students

While attempts to exclude unsuitable on-line material from schools invoked narratives of the "student-at-risk" and the "dangerous student", efforts to exclude

students from the Internet arguably reflected a concern for the well being of the institution. Two distinct approaches to excluding students from the school Internet were evident in the research. The first approach, which focused on limiting initial student access to the machines, included such measures as locking rooms, limiting the number of machines that could access the Internet, using passwords, introducing Internet booking procedures and ultimately disabling Internet access. The second approach centred on expelling students from the Internet, IT suites and ultimately the school. In considering these two approaches to excluding students, I will focus in turn on primary, secondary and post-16 institutions.

2.1 Primary schools

Although both Avenue and Brooklands primary schools had a security system that meant visitors had to speak through an intercom before the main entrance was unlocked, within the school there was no evidence of rooms being locked during the day. While no reason was given for this relaxed in-school security, the small number of rooms, the low number of total students and the relatively high level of staff supervision could all be considered significant factors. This situation potentially allowed students to access Internet machines throughout the whole day.

Cliff, the Head of Brooklands was asked whether he had considering restricting the number of Internet machines to keep a tighter control of on-line use. He argued that he was a keen advocate of giving powerful computing machines to children and maintained that he saw no real benefit in prohibiting older students from accessing such technology.

One of the ways in which student access was controlled at both Avenue and Brooklands was with passwords. In the primary schools, not all children had passwords that gave them access to the Internet. Rather students had passwords that gave them different levels of access to the school network, with only the older students having Internet access. When asked why students in the reception class were restricted from using the Internet, Cliff replied, "simply because of the

non-selective way in which they use computers. They just click on something, point and click, click and click and click again" (Cliff, Head, Brooklands).

The effectiveness of such a control system was largely dependent on the passwords remaining secret between year groups. At Brooklands Jo, the ICT co-ordinator, described how she had found a young student "surfing" for cartoon websites although his password didn't allow Internet access. Upon questioning him, she discovered that this student had watched his older sister at the school enter her Internet password and had made a note of it.

During the research process, no primary school students were observed being told to log off the Internet, or leave the room. Neither were there reports of students being suspended or expelled for Internet misuse.

Overall the use of passwords to exclude students from the Internet in primary schools can be seen as primarily concerned with protecting students from accidentally accessing unsuitable material. According to Cliff the Head at Brooklands the risk of younger students unintentionally accessing unsuitable material was high insofar as they were indiscriminate "surfers", constantly clicking on icons with no real conception of the websites they might access. Furthermore, as no incidents were reported where student Internet access was withdrawn, it appeared that younger students might not engage in on-line activities that threatened the school. Overall the policy of excluding younger students from Internet use at both Avenue and Brooklands primary school can be seen primarily as an attempt to protect the "student-at-risk".

2.2 Secondary schools

Locking rooms with Internet access was a control strategy adopted in all five secondary schools. At Canalside following a spate of vandalism, in which computer hardware was damaged, IT rooms were locked unless a teacher was present. At Dalehouse IT classrooms were locked when a member of staff was not present to "prevent general abuse of computers and the Internet in particular" (Dave, ICT manager, Dalehouse). After students "hacked" into the school

Intranet at Eastway Mary, the Head of IT, explained that classrooms with Internet connections were to be locked unless a member of staff was present. At Forestfields Kate, the ICT co-ordinator, related how all IT rooms were locked "partly for health and safety reasons, partly so that young students can't get unsupervised access to the Internet" (Kate, ICT co-ordinator, Forestfields). While the ICT manager at Greenswold attempted to provide Internet access on as many computers as possible, he was still able to control use of these machines by locking the rooms in which they were situated. Indeed despite having access to over one hundred Internet machines students were largely unable to use these facilities at break times as the rooms remained locked due to a lack of staff to supervise. This illustrates how one control strategy such as surveillance can potentially replace another one such as exclusion. Robert, the ICT manager at Greenswold explained the reasoning behind locking rooms with Internet access by arguing that "the students can't get up to mischief on the Internet if they can't get into the rooms that have Internet access" (Robert, ICT manager, Greenswold).

None of the five secondary schools sought to deliberately limit the number of machines that were connected to the Internet. Rather there was a tendency for schools, such as Dalehouse, Forestfields and Greenswold to seek to provide as much Internet access as possible. At Dalehouse, Zed, the ICT co-ordinator discussed plans to effectively turn the school library into a cyber-cafe after the end of the school day. He actually suggested that they could serve coffee and other hot beverages. The reason put forward for the creation of this cyber-cafe was to encourage students and parents to use the Internet. Students were encouraged at Forestfields to use the Internet outside school hours and a computer club briefly ran on Friday evenings. At Greenswold a "Cyber-Dad" program was set up enabling students and their fathers to come into school on Saturdays to use the Internet.

At all secondary schools, students were given personal passwords that allowed them to log onto the school network and use the Internet. However, insofar as all students' passwords gave access to the Internet this could not be seen as an attempt to exclude students. Rather in secondary schools passwords tended to be

used to record the websites visited. This issue of surveillance is considered in detail in the next chapter.

Some form of reservation system was in existence at Canalside, Dalehouse and Forestfields. In theory these systems restricted the amount of time students could use the Internet outside of lessons. While at Canalside and Dalehouse lunchtime Internet use was clearly designated for particular groups at Forestfields a booking system was in effect. At Canalside, Internet use in the ICT suite was restricted to female students one lunchtime a week. According to Wilf the IT Head this was to counter the tendency for boys to be more forceful in securing computer use. As the lunch time session was supervised by staff this system appeared to be effective in restricting boys' Internet access and encouraged girls to use the machines. Indeed during the three such sessions that I observed, all of the eighteen computers were used by girls. Yet as Wilf remarked this policy was not really about controlling boys' Internet activities but more about "giving girls a fair chance to use the Internet" (Wilf, IT Head, Canalside). Indeed, there were two other computer suites in the school to which the boys could try and gain access. At Dalehouse lunchtime Internet access was designated each day for particular year groups. Yet, as the machines were never fully occupied the librarian declared that she saw no harm in "bending the rule". Indeed some students were observed using the Internet in the library at lunchtime, day after day, regardless of their designated period of "surf time". Students at Forestfields, were required to book a computer if they wished to use the Internet located in the Learning Resource Centre. Yet, no evidence of advance booking was observed. Rather students found a free computer and logged onto the Internet, only retrospectively booking their Internet session when the librarian informed them that they had to sign the book if they wanted to use a computer. During one lunchtime the librarian's reminder that students needed to book Internet machines caused a rush towards the log book of year eight male students who had already managed to secure a computer but had failed to sign their names. That this booking system was used as a reference source to keep track of who used which machines was indicated by the librarian asking on-line students their names and entering them in the log book even when the room was almost empty.

Reservation systems in the secondary schools focused upon allowing all students equal access to the Internet rather than excluding some students from on-line activity. While it might be argued that an unintended consequence of reservation systems was to limit access for the "technophile" student who sought to spend as much time as possible on-line there was no evidence to suggest that this occurred in Canalside, Dalehouse or Forestfields.

The most extreme reported method of excluding students from Internet use was disabling the software so that they could not log onto the 'net'. While this action was wholly effective in stopping school Internet misuse, it also eradicated the possibility of educational gains. This was not a policy advocated in any of the secondary schools. However, it was used as an emergency measure for three days at Greenswold after the Internet service providers filtering system crashed. As Robert, the ICT manager noted:

> The filtering went down as well one time which was embarrassing ... they [students] typed in sex.com and up it came. Which caused a few days of trouble, we had to switch the machines off (Robert, ICT manager, Greenswold).

With regard to the expulsion of students, in all five secondary schools students were observed being told to log off the Internet and leave the room. Sometimes this request was made calmly by staff, whilst upon other occasions it involved shouting and displays of staff anger. Thus, students were seen in Canalside, Eastway, Forestfields and Greenswold being told to log off the Internet after they had been caught on chat-lines. At Dalehouse where chat-lines were allowed, students were observed being thrown off the Internet for failing to work during lesson times. While students being told to log off the Internet was a common sight in all five secondary schools, none of these schools reported suspending or expelling a student for Internet misuse.

At Canalside, Eastway, Forestfields and Greenswold students were banned from using the Internet from periods ranging from two weeks to a term following incidents where they had intentionally accessed pornographic material using the school Internet. Mary, the IT Head at Eastway, explained how she had wanted to

ban sixth form students who had "hacked" into the school system from the Internet. Due to parental pressure and practical considerations the students went unpunished. While no Dalehouse students were banned from using the Internet, Dave, the ICT manager, declared that they would be barred from on-line activity if they were caught "hacking" into the local network.

Overall, secondary schools adopted policies of locking rooms with "net" access, using passwords, introducing reservation systems and upon one occasion disabling the Internet system. However, neither the adoption of passwords nor the use of reservation systems should be seen as measures to exclude students from Internet use. Passwords were used in the secondary schools for surveillance and to provide a degree of accountability for "surfing" activities. While the reservation systems introduced at Dalehouse, Canalside and Forestfields potentially provided all students with a chance to use the Internet, they did not restrict the "surfing" activities of students who sought to go on-line on a daily basis. Nevertheless, locking rooms and disabling the Internet system could be seen as effective strategies of excluding students from on-line activities. Arguably, both of these policies were used in secondary schools primarily to deal with threats posed by "dangerous students". Hence locking rooms stopped students from vandalising Internet machines or getting up to "mischief" on-line. The disabling of the Internet at Greenswold was a direct result of the filtering software crashing and students intentionally accessing the sex.com website.

With regards to temporary expulsion as a method of Internet control, students were seen in all five secondary schools been thrown off the "net". Furthermore, at Canalside, Eastway, Forestfields and Greenswold students were barred from going on-line for a set period after having accessed pornographic material. These general acts of expulsion were a response to students intentionally misusing the Internet to access items such as chat-lines or pornography. Arguably, in this sense such acts were not primarily concerned with protecting the "student-at-risk" but rather with safeguarding the institution from the on-line activities of the "dangerous student".

2.3 Post-16 institution

At Hightree there were twenty-four computers in the main IT suite, with twelve positioned each side of the room. Although all twenty-four computers could be linked to the web only one side of the room, that is twelve computers, were Internet enabled at any one time. According to Tony the ICT manager the main reason behind this policy was to make it easier to control student access and on-line activities. Jim, the Head of science, agreed that limiting the number of Internet computers allowed for greater control, adding that:

> We purposely left it at 12 [Internet machines] because we didn't want the whole resource centre turning into a cyber-cafe. It also allows the rest of the machines to be used for project work (Jim, Head of science, Hightree).

Not only is it suggested that effective Internet control is related to the number of machines students can access at any one time, but Jim's fear of the resource centre turning into a cyber-cafe, suggests that he believes that students will use the Internet for recreational communication, even though chat sites were prohibited.

A booking system limiting each student to one-hour of Internet access per day was introduced at Hightree. This policy arose following Tony's examination of the school computer logs which showed "names that were cropping up 8.30 in the morning, might go off and on a little bit, but they were basically there towards the end of the day" (Tony, ICT manager, Hightree). The booking system took the form of a written record, that students signed to reserve one-hour blocks of Internet use. Problematically Tony noted that some students were booking vast amounts of time on the Internet as far as two weeks in advance. Arguing that the booking system was generally ignored Kylie, a year twelve student, explained "we're only allowed to use it [the Internet] for about an hour, but we use if for longer. About two or three hours" (Kylie, year 12, Hightree).

Passwords were used at Hightree to gain access to the college network. Yet, they were primarily used as part of the process of surveillance rather than to restrict "net" access. One student who refused to sign the college Internet Acceptable

Use Policy was an exception to this situation. He was not given a password and therefore was denied access to the school system.

As in the secondary schools it was not an uncommon experience at Hightree to see students being told to log off the Internet and leave the room when staff caught them misusing the Internet. However, a student at Hightree was actually expelled for accessing what was labelled as pornographic material. According to Jim, the Head of science, it was felt that any long period of suspension would damage the student's academic development, whereas expulsion allowed the student to immediately enrol in another institution and continue his education without pause.

Overall, limiting the number of Internet machines and introducing a booking system can be seen as attempts to control student Internet access at Hightree. Yet, it would be difficult to argue that these were effective exclusion policies. After all, despite the limit on Internet machines in the main IT suite and a booking system students still managed to spend large periods on-line on a daily basis. Expelling students both from the Internet and in one case from the school could be seen as strategies intended to exclude "dangerous students" from Internet use. Both these measures were described by staff as responses to students intentionally misusing the school Internet.

2.4 Summary

While the primary schools sought to use passwords to exclude and protect students perceived as being at risk, secondary schools used a wider range of policies largely concerned with safeguarding the institution from the "dangerous student". In the post-primary schools, locking rooms and disabling the Internet system proved effective in excluding students from on-line activity. Indeed both these practices could be seen as responses to the "dangerous student". Thus fear that students would vandalise computers or get up to mischief on-line led to the locking of rooms that contained Internet machines in all five secondary schools. Furthermore, the Internet was disabled at Greenswold for three days after the

filtering software crashed and students intentionally started accessing pornographic websites.

All the post-primary schools also made use of expulsion strategies to control student Internet use. Thus in all these institutions students were seen being ejected following incidents where they had been caught misusing the Internet. Additionally at Canalside, Eastway, Forestfields and Greenswold students were barred from on-line activity for a set period after they had been caught accessing pornography. Indeed, at Hightree one student was expelled from college for viewing pornographic material using the school Internet. All these incidents of exclusion have in common a concern with the dangerous, intentional activities of students. In none of the schools was a student seen or reported as being excluded from "net" use following an incident where they had accidentally accessed unsuitable material. In this sense the strategy of excluding students from Internet use in the post-primary institutions could be seen as a reflection of concern with the "dangerous student".

Limiting the number of Internet enabled machines, using passwords and introducing reservation systems in post-primary schools could be seen as general control strategies which were largely concerned with facilitating the use of resources for all students. Indeed, only Hightree deliberately limited the number of Internet machines with the declared intent of seeking to control student Internet use. In the post-primary schools passwords were used primarily as surveillance tools rather than to restrict Internet access. Reservation systems were used in Canalside, Dalehouse and Forestfields to provide opportunities for all students to use the Internet. Only at Hightree was the booking system introduced with the declared intent of prohibiting excessive Internet use.

Conclusion

Schools in the research used a variety of policies to exclude on-line material and students. While in the primary schools these actions were taken primarily to protect students from on-line dangers, in the secondary and post-16 institutions such strategies reflected an anxiety with the on-line activities of the "dangerous

student". Indeed while in the secondary schools excluding material was seen as an approach which both protected the student and the institution, excluding students was an activity largely concerned with protecting the school from the on-line activities of the "dangerous student". In the post-16 institution Tony the ICT manager had identified policies of both excluding material and students as being primarily concerned with safeguarding the institution. In seeking to elaborate upon these points, I will briefly review how the primary, secondary and post-16 institutions sought to control Internet use through exclusion.

In the two primary schools "deny lists" and keyword-matching software was used to exclude unsuitable on-line material. In addition, passwords were utilised to stop younger students from accessing the Internet. Staff discussed the exclusion of on-line material and of young students in terms of the need to protect students. Suggestions that such activities might also protect the institution from "dangerous students" were rejected as irrelevant by staff.

A variety of exclusion policies were used in the secondary schools to control Internet use. Thus all five secondary institutions used "deny lists" and keyword matching to exclude undesirable material. Additionally Canalside and Forestfields used a graphic content management application that blocked images containing large amounts of skin tone. Observations and interviews suggested that these filtering packages were intended to shield students from unsuitable Internet material and to protect the institutions from the on-line activities of the "dangerous student". Although the secondary schools used a variety of methods of Internet control some of these, such as reservation systems and passwords were not primarily intended to exclude students. Indeed reservation systems were introduced to ensure Internet access for all students, while passwords were used mainly as a surveillance tool. Locking rooms, disabling the Internet system, throwing students off-line and barring them from the Internet were all policies that effectively excluded students. Thus in all secondary schools it was not an uncommon occurrence to see students ejected from machines for accessing chat-lines or other websites deemed unsuitable by staff. Furthermore, at Canalside, Eastway, Forestfields and Greenswold students were prohibited from using the school Internet for a period of time following incidents in which they had

intentionally accessed on-line pornography. Such actions were reportedly intended to protect the educational institutions.

In the post-16 college filtering software utilising "deny lists" and keyword matching was employed. Staff also sought to control Internet use through limiting the number of machines linked to the web, the use of passwords and the introduction of a booking procedure. Students were seen been told to log off the Internet after accessing unsuitable websites. Furthermore one student was expelled from the college following an incident in which he accessed a pornographic image. The exclusion of both Internet material and students were reportedly motivated by the desire to protect the institution from intentional Internet misuse. This was explained by Tony the ICT manager who maintained that as the students were young adults safeguarding them from unsuitable material on the web was a lesser concern, compared with protecting the institution from the effects of their mischievous actions.

It can be seen that the age of the student was an important determinant of whether staff invoked the narrative of the "student-at-risk" or the "dangerous student". While in primary schools exclusion policies were primarily concerned with protecting students, in the secondary schools safeguarding the institution was also a concern. Indeed, in the post-16 institution the exclusion of material and students was used primarily to protect the college from the on-line activities of the "dangerous student".

A key factor in the effectiveness of exclusion as a form of Internet control is surveillance and it is this subject that I consider in the next chapter. Thus I will examine some theoretical writings on surveillance before focusing on schools' attempts to physical and virtually observe student Internet activity.

Chapter Eleven

Surveillance and the school Internet

Introduction

In the previous chapter, I considered how schools sought to control Internet use and alleviate risks, by excluding unsuitable material and "dangerous students". To curtail students' unsuitable "surfing" activities and hold them accountable for their on-line actions, staff need to able to observe student actions. In this chapter, I consider attempts to control student Internet use through surveillance. Thus I focus upon the concept of surveillance before exploring the forms of physical and virtual observation used in the fieldsite schools.

In seeking to outline the issue of surveillance, I first consider the writings of Foucault on panopticism. I then turn to Ball's work, which asserts that surveillance fosters accountability while encouraging social order. Finally, I ponder how these general ideas can be applied to a consideration of surveillance of Internet use in schools. In particular I focus upon the threads of physical and virtual surveillance.

With regards to physical surveillance I argue that three issues need to be addressed, namely the identity of the observer, the focus of the observation and the use of space. I consider each of these issues in detail before examining how physical observation of Internet use was undertaken in the primary, secondary and post-16 institutions. I conclude that while surveillance in primary schools appeared to be concerned with the "student-at-risk", in post-primary schools the focus rested upon the activities of the "dangerous student".

In the fieldsite schools two forms of virtual surveillance applications existed, programs that recorded the addresses of websites accessed and software, such as Net Top Teacher, which allowed staff to view and control student Internet activities. While two schools in the research owned these latter devices, they were not actually used as surveillance tools. Having described the virtual

surveillance methods available to schools in the research I note that such observation tended to rely on computer logs of websites visited. Although computer logs existed in the primary schools, staff claimed that they were not used. This was explained with reference to the behaviour of on-line students and a lack of concern about the intentional accessing of unsuitable material. However, in the secondary and post-16 institutions computer logs were used to reconstruct incidents of Internet misuse, identify those who accessed unsuitable websites and hold them accountable. These arguments lead me to conclude that virtual surveillance in post-primary schools represents an attempt to control the activities of the "dangerous student".

It should be noted that occasionally I use information that casts doubts upon the effectiveness of certain methods of surveillance. My purpose in this research is not to offer a comprehensive assessment of the effectiveness of surveillance. Rather I present the information merely as an initial indication of problems that may emerge in attempting to use surveillance to control Internet activity. Before considering physical and virtual surveillance, I will examine the concept of surveillance.

1. Surveillance

Reflecting upon the concept of surveillance, I will first focus on Foucault's work on panopticism. While I note that self-surveillance is a central element of panopticism I argue that it is difficult to assess in a school setting, hence I concentrate on the more distinguishable aspects of general surveillance. Drawing upon the arguments put forward by Ball I note that systems of surveillance potentially foster accountability and encourage social order. Finally, I consider the ways in which surveillance in broad terms might act upon students using the school Internet.

In 1791, the utilitarian philosopher, Jeremy Bentham, published the design for a prison called the panopticon; a postscript to the design was published later in the same year. It is in the postscript that the diagram taken as illustration by Michel Foucault in *Discipline and Punish* (1977) and Thomas Markus *in Buildings and*

Power (1993) can be found. The fundamental principle of the panopticon is observation from a central point towards the activities of the people at the parameter. In Bentham's design prison cells situated around the periphery of the building face inwards towards a darkened central watchtower. The cells are exposed and backlit so that their occupants can always be seen from the central tower. However, the watchtower is darkened so that prisoners looking inwards towards the tower can not be certain if they are the object of observation. The peripheral mass cannot see their observers and must assume that they are the subjects of constant surveillance. Bentham referred to this arrangement as the "Inspection House", claiming that its design would "invigorate industry", "reform morals" and "facilitate education". The panopticon was very different from its carceral predecessor, the dungeon. Rather than abandonment in darkness, the prisoner in Bentham's design is subject to permanent display, as Thomas Markus notes he is "seen but he does not see: he is the object of information, never the subject of communication" (1993: 200). The panopticon disassociates power from particular people, investing it in a configuration of light, inspection and architecture. In this context, observation comes to be perceived as continuous. This in itself comes to control the behaviour of the prisoners.

For Foucault the core of panoptical society was the monitoring of the activities of a large group of people by a small number of individuals who acted on any infractions of the required behavioural regime. This would appear to be a powerful model for social analysis. It can be claimed that in contemporary society welfare administration, police control, commercial activities and formal education all display some aspect of panoptical control. Key to Foucault's idea of the panopticon is the notion that those on the periphery are never totally sure if they are being observed at any one particular moment. In this situation, the rational individual seeking to avoid punishment for infringement of a social code must act as if they are the object of current surveillance. This state of affairs effectively gives rise to the situation where individuals begin to police themselves through the operation of ways of thinking and behaving which define what is normal in society. The shaping of behaviour is thus established through

discourses by which individuals channel their behaviour into socially acceptable forms.

However, in the schools in which this research was undertaken it was difficult to empirically assess the extent to which students practised self-surveillance. While I would maintain that, with regards to school Internet use, elements of panopticism existed, the difficulty of evaluating such matters led me to concentrate on the more visible aspects of surveillance. After all, panopticism is concerned with effective observation of peripheral objects from a central location. To consider such activities purely in terms of self-surveillance ignores a key element of this phenomenon. Thus, I will focus largely on the issue of effective surveillance of Internet use, although where appropriate I will make reference to issues of self-policing.

On a basic level, surveillance provides the observer with information about the activities of the observed. If an observer sees an individual transgressing institutional rules or wider social norms then they might choose to pursue disciplinary action, possibly seeking to confront and punish the transgressor. Such action reinforces social order, by reminding individuals of rules and norms, while confirming that people are generally accountable for their own actions. Thus, if a student was seen using the school Internet to access prohibited material, then they might be confronted and punished. Surveillance plays a central role in this process, insofar as an offence must be seen to have taken place before action can be taken to punish the miscreant.

In some circumstances, the observed will be aware that they are the object of surveillance. Drawing upon the work of Ball (2000) it can be argued that individuals might modify their behaviour if they are aware that they are being watched. After all, an awareness of being observed can remind individuals of social rules, while offering the possibility of accountability and punishment for social transgressions. Students who are aware that staff are watching their on-line activities might arguably be reminded not to access prohibited websites, if only for fear of being held accountable and punished.

Ball (2000, para 1.2) notes that surveillance systems are items of material culture which are capable of effecting a modification in the behaviour of persons within a clearly defined area. Hence, they are in large part installed to promote an element of social order and accountability within an environment. After all, order is a product of how other people interact both with other persons and objects, including inanimate items of material culture such as surveillance systems. If surveillance systems are visually evident, they serve to remind individuals of rules and promise accountability, in that any transgression might be recorded and acted upon.

In addition to introducing an element of accountability and enforcing social order, surveillance can also provide entertainment. This aspect of surveillance has grown in recent years with the emergence of "reality TV" shows such as *Big Brother* where contestants are the subject of constant observation. Yet, there was no evidence in the research that surveillance in schools fulfilled an entertainment role. Rather observation was concerned with social order and accountability.

Having explored the issue of surveillance and how it engenders accountability and self-policing I will consider the observation of Internet use in the eight schools involved in this research. Drawing upon the narratives of the "student-at-risk" / "dangerous student", I will focus in turn upon physical and virtual surveillance.

2. Physical surveillance

In schools if staff wished to ensure that students do not misuse the Internet they could simply observe their activities. Such surveillance gave rise to control insofar as students were aware that they were observed, recalled institutional rules regarding Internet use and were reminded of the possible punishments for misuse. Furthermore staff could punish students for any observed transgression. Before considering examples of physical surveillance relating to Internet use in the fieldsite schools, I will address issues questions that are relevant to the subsequent discussion. Namely, the identity of the observer, the focus of the observation and the use of space.

While teachers were expected where possible to supervise their own students' use of the Internet, the provision of Internet access in libraries and specialist ICT suites also meant that both librarians and technicians often became involved in watching students' on-line activities. Furthermore as Internet access in schools was often centrally situated, in a main library or ICT resource centre, staff who wandered through these rooms could also peruse students' on-line activities. Watching children using the Internet was not just an issue of control, rather as Kate the ICT co-ordinator at Forestfields noted, it was also a health and safety issue. Thus she remarked:

> On the whole, years 7 to 11, there's got to be a member of staff in the room. Not so much for the surveillance of what they're doing on the machines but it is more the health and safety side, in case there is an accident in the room (Kate, ICT co-ordinator, Forestfields).

While it can be recognised that staff fulfil a central role in the physical surveillance of school Internet use, the part played by students should not be ignored. Students watching the activities of their peers might choose to draw staff attention to unsuitable "surfing". Even if they choose not to act if they see someone accessing unsuitable on-line material, they can still potentially be called upon as witnesses.

Overall, a wide range of staff carried out physical surveillance in schools, including teachers, librarians and ICT technicians. Furthermore, there existed a degree of peer surveillance as students observed one another's on-line activities.

Traditionally the focus of observation in school has been the student's body. In particular teachers sought to observe students' faces to see if they were talking, or to provide an indication of emotions. With regards to the school Internet, the focus of surveillance upon an individual remains useful, insofar as displays of personal excitement or attempts by a student to conceal a screen indicate that something worthy of note might be occurring. Yet, with computer use the primary focus of surveillance is often the monitor screen. The screen provides the best insight into the on-line activities of students. Arguably, in many schools with the introduction of information communication technology, there has been a

shift in the surveillance focus from the face of the student to the computer screen. Thus, many classrooms have computers along the walls facing inwards to the centre of the room, rather than in rows. This means that the computer screens are more easily visible to teachers in the centre of the room.

Yet physical surveillance of Internet use in schools does not just focus on individual / group behaviour or the computer screen. Rather, staff might also concentrate on printed material, close circuit television cameras and the amount of work done by students. If students access unsuitable material on the school Internet then it is possible that they might attempt to create a print copy. By observing the material that is printed staff can indirectly keep a check on the websites visited by students. As Ball (2000) notes, there has been a growth in the use of CCTV cameras, not least in educational institutions. While traditionally surveillance cameras were focused upon the world outside the school recording acts of vandalism or attempts to break into buildings, with the introduction of expensive ICT equipment into schools CCTV cameras now focus inwards. Thus, staff can observe student activity in real time on a CCTV screen or even review previously recorded material. Finally, teachers might adopt a strategy of filling student time, by setting work and then seeing how much of the task the student has completed in a set time. A typical example of this situation is where a teacher might send a student to the ICT centre to use the Internet with instructions to complete a set amount of work and then return to the classroom. By checking that the work has been done the teacher exercises a degree of surveillance. Overall then the focus of surveillance of Internet use might vary from the activities of the students to the computer screen, printed material, CCTV screens and the work done.

The issue of positioning computers so that teachers can easily see the screens has already been touched upon. Central to the concern of screen visibility is the use of space. In order to realise the power inherent in surveillance, the observer must be able to see the object of interest. The ability of teachers to observe students' computer screens depends upon the use of space. I have already suggested that computer screens can be effectively observed from a central position if they face inwards, towards the centre of a room. In a sense, this spatial geography mirrors

that of the panopticon, with the teacher replacing the central watchtower and computer screens being substituted for back-lit prison cells. However, surveillance of Internet use is not the only concern in schools. The dynamics of economics and limited classroom space might dictate that as many computers as possible be packed into a room. This aim might be at odds with ensuring that computer screens are easily visible from a central location in the room.

The identity of the observer, the focus of observation and the use of space are issues that I will consider in describing the physical surveillance of Internet use carried out by the schools in this research.

2.1 Primary schools

At both Avenue and Brooklands primary schools staff claimed that students using the Internet were always supervised. While the task of physical surveillance fell to teachers during lessons, the ICT co-ordinators tended to supervise on-line activity outside normal lesson times. Additionally, part-time staff were brought in to supervise lunchtime activity, which included watching students activities inside the classrooms as well as outside in the playground. Discussing students need for supervision, Cliff the Head at Brooklands remarked:

> I wouldn't see it [using the Internet] as appropriate for a group of unsupervised children on a wet playtime. That would be highly inappropriate. There's supervision issues. We are responsible for the children's welfare. They should be supervised anyway but if students are using the Internet then staff need to be more aware of what the students are actually doing (Cliff, Head, Brooklands).

Cliff noted the general need for supervision of students that existed within schools, while highlighting that those using the Internet should perhaps be monitored more closely. Indeed during my periods of observation at both Avenue and Brooklands primary schools, staff were always present within classrooms when students were "surfing" on the "net". Of course, this in itself was no necessary indication that staff were always keenly observing students' on-line activities. As students tended to use the Internet in both schools in pairs or small groups, there was often a degree of peer surveillance of student Internet activity.

Ella the ICT co-ordinator at Avenue remarked that where possible she preferred students to use the Internet in small groups. Talking about students collaboratively using the Internet she explained "we're making the most of our resources, more students get Internet experience, they can help one another, learn to work together and they can sort of keep an eye on each other" (Ella, ICT co-ordinator, Avenue). Ella highlighted that there were some sound educational reasons for encouraging students to use the Internet in small groups, adding that such an approach also involved an element of peer surveillance. At Brooklands primary school, students were seen sharing Internet machines, even when other networked computers were vacant.

In both Avenue and Brooklands primary schools there were two or three Internet linked machines in each of the main classrooms. The machines were positioned against the wall so that their screens faced inwards towards the centre of the room. When asked whether the placing of the Internet-linked machines had been a conscious decision, Jo the ICT co-ordinator at Brooklands replied:

> Well it was really a question of space and where we could fit the machines and all the wiring. But I guess it was important that the screens were clearly visible, not hidden. So that we could keep an eye on the students (Jo, ICT co-ordinator, Brooklands).

While Jo recognised space restrictions in the classroom, she nevertheless noted that the screens should be clearly visible to supervisors. Indeed Ella, the ICT co-ordinator at Avenue shared a similar view noting that "we wouldn't have put the Internet with the screens facing into the corner. We want to be able to see student activity, not conceal it" (Ella, ICT co-ordinator, Avenue). Such considerations highlight the importance of the computer screen as the focus for physical surveillance of student on-line activity.

While staff surveillance in Avenue and Brooklands focused on the computer screen, there was also evidence that the printing of items from the World Wide Web was observed. Jo, the ICT co-ordinator at Brooklands, complained about students printing material from the web.

> You've got to watch them [students] because they'll print stuff indiscriminately off the web. So, you might have ten pictures of Leonardo DiCaprio clogging up the machine. We tend to keep a tight rein on what they print (Jo, ICT co-ordinator, Brooklands).

At Brooklands, the school only had one printer to which all the computers were linked. This meant that the printing of pictures from the web held up other student's work. Thus, Jo explained that she kept an eye on what was printed. While there was more than one central printer at Avenue Ella also noted that she observed students printed output from the web. Although in this case Ella's concern also related to the expense of using a colour printer. Neither of the schools had CCTV cameras installed inside the building.

In summary, both teachers and lunchtime staff supervised Internet activity in the primary schools. There was also a degree of peer surveillance arising from a group work approach to Internet use. The Internet machines were positioned so that their screens could be easily viewed from the centre of the classroom. In addition to staff watching computer screens, they also viewed material that was printed by students from the web. In discussing the degree of physical surveillance of student Internet use, I suggested to Cliff the Head of Brooklands that staff might be concerned with students intentionally accessing unsuitable material. He replied:

> The students behave themselves, so we're not so much bothered about them deliberately misusing the Internet. It's more if they accidentally stumble across something ... unsuitable websites, then if staff are immediately aware, they can act (Cliff, Head, Brooklands).

Ella, the ICT co-ordinator at Avenue echoed this sentiment, arguing that there was a need to watch students on-line because they were potentially at risk and would require help if they stumbled across unsuitable material.

2.2 Secondary schools

In all the secondary schools in the research a range of staff were involved in observing Internet activity, including teachers, librarians and ICT technicians. In

Dalehouse, Eastway, Forestfields and Greenswold secondary schools, where Internet provision was situated in or near the library, the main task of physical surveillance fell to the library staff. Thus at Dalehouse library staff were seen circulating around the Learning Resource Centre making sure that students who used the Internet behaved in an appropriate manner. Indeed, at Forestfields one of the main jobs of the librarian, Liz, was to observe Internet use and ensure that students were not accessing unsuitable sites. In Eastway and Greenswold the library was connected to the main rooms providing Internet access and library staff were seen almost constantly circulating and observing student on-line activity. At Canalside the main Internet access was situated in the computer suites rather than the library. Indeed only two non-networked computers were placed in the library. As a result much of the supervision of Internet use was carried out by IT teachers and technicians. However, during lunch periods other teachers at Canalside were seen helping ICT staff supervise student on-line activity. In all the secondary schools teachers who booked an ICT room to use with a class were responsible for supervising the group. At Dalehouse, Eastway, Forestfields and Greenswold where teachers sent small numbers of students from their lessons to use the Internet situated in the Learning Resource Centre, the task of surveillance fell to the library staff. In addition, in all five schools staff were observed passing through resource centres and ICT rooms, taking an interest in the "surfing" activities of the students. Indeed at Forestfields I observed a member of staff who was passing through the resource centre, stop to reprimand students who were using the Internet recreationally, before continuing on his way.

In all five secondary schools in addition to staff physically observing Internet use there was also an element of student peer surveillance. Thus, students were seen watching one another "surf". When a student at Dalehouse accidentally downloaded a picture of a bikini clad female wrestler three male students quickly gathered around the computer screen. At Greenswold, the discovery of an on-line game called "Cowfighter" resulted in an excited gathering of several year eight students around a computer screen, while the student responsible for accessing the site frantically tried to log off the Internet. Kate, the ICT co-ordinator at Forestfields argued that students fearful of losing Internet privileges would

observe one another's "surfing" activities to ensure that there was no misuse of school resources. Indeed at Forestfields some sixth form students acted as monitors, with supervisory powers over students' Internet use in the Learning Resource Centre.

In summary teachers, librarians and ICT staff were involved in physical surveillance of Internet use in the five secondary schools in the research. Although students also observed one another's on-line activities, it was not always apparent whether they would report incidents of Internet misuse. However, at Forestfields the system of student peer surveillance had been formalised, with sixth form students supervising Internet use in the Learning Resource Centre after school.

While computer screens that face inwards towards a central focal point in a room facilitate surveillance, such a formation is not always an economically effective use of space. Rather economic efficiency might dictate as many Internet machines as realistically possible be installed in a room. Such spatial economics may lead to the positioning of computers in rows rather than in circles. At Canalside, Dalehouse, Eastway, Forestfields and Greenswold surveillance issues arguably came second to economic considerations. At Canalside computers were situated in figure eight formations, effectively dividing the ICT rooms into two circles. Some Internet computers at Dalehouse were placed in the Learning Resources Centre in broken rows. At Eastway the Internet computers were positioned in rows, while at Forestfields and Greenswold some machines were placed back to back so that a greater total number could be placed in a room.

At Canalside Wilf, the IT Head, noted that "it's a trade-off really, we try and fit as many computers as possible into a room but still try to ensure that teachers can easily see the monitor screens" (Wilf, IT Head, Canalside). Hence, despite the pressure to fit as many Internet machines as possible into a room it was still recognised that screen visibility was an important issue. The following discussion with Dave the ICT manager at Dalehouse served to illustrate the importance of screen visibility:

Interviewer: Was screen visibility a factor when you were setting up the computers?
Dave: Yes it was essential that we could see the screens of the computers that the Internet was to be on.
Interviewer: How is the business suite set out?
Dave: The computers are mostly around the edge, facing inwards. There's just one machine that doesn't, you have to be careful who you sit.

Hence Dave highlighted the importance of being able to see students' computer screens. Indeed he suggested that in the business studies Internet suite teachers had to be careful which student they placed at the one screen that was not easily visible. At Eastway Mary, the Head of IT, noted how mischievous students tended to seek out computers with screens that were not easily visible from anywhere else in the room. Indeed, she related that a student who "hacked" into the school Intranet had used a computer situated in a corner with a screen that faced the wall. According to ICT staff at both Forestfields and Greenswold students caught accessing pornography on the school Internet, had used computers whose screens faced towards the wall and were not easily visible from anywhere else in the room. Arguably such incidents indicated that students were aware of the importance of screen visibility in ensuring effective physical surveillance of Internet use.

In the secondary schools physical surveillance of Internet activity was not restricted to watching student computer screens, rather staff also focused upon material printed from the web and the amount of work done by students.

The printing facilities in the Learning Resource Centre at Forestfields were switched off as the librarian left at the end of each day. As a printing credit system was in operation this was not done in response to the fear that students would print excessive amounts of material. Instead Liz the librarian argued that it was an effective way of observing and controlling what students printed. At night with the printer shut down the system stored up the print jobs so that she could peruse them in the morning before switching the printer back on. Liz declared that if she found unsuitable material in the printing requests she would delete it, though she never clarified how she would know it was unsuitable without first printing it. Although switching the printer back on was a relatively simple

procedure, none of the students who stayed behind after school were observed doing this. At Greenswold Robert, the ICT manager, noted that he and the library staff watched the material that was printed. Indeed according to Robert, one student who had accessed pornographic material using his friends Internet password had printed off an image knowing that staff would see it and seek to find the person responsible. At Canalside, Dalehouse and Eastway concern about printing material from the Web was focused as much upon the misuse of limited school resources as it was upon the creation of hard copies of unsuitable material. Zed, the ICT co-ordinator at Dalehouse, related, "we keep tabs on the printing of stuff from the Internet because most of it's a waste of resources, wrestlers, pop stars ... it's not so much fear that they're printing porn." (Zed, ICT co-ordinator, Dalehouse). At Eastway Mary the IT Head noted how "we try and control printing to stop students printing these huge, many paged, hyper-text documents" (Mary, IT Head, Eastway). Wilf, the IT Head at Canalside, also noted the necessity of watching what students printed from the web, complaining that they often selected items without any consideration of length or relevance to their work, "tying up the printer" (Wilf, IT Head, Canalside).

Teachers also monitored student Internet activity at Canalside, Dalehouse, Eastway, Forestfields and Greenswold by setting work that filled students' time and then checking it was completed. This strategy tended to be used by staff who sent students individually or in small groups out of a lesson to use the Internet in the Learning Resource Centre. At Canalside I talked to three year eight students who were eager to finish their on-line tasks so that they could return to class and show their teacher their work. In Dalehouse LRC one boy waiting by the printer told another student that he had to print the material he was working on or when he returned to class the teacher wouldn't believe he'd done the work. Mary the Head of IT at Eastway remarked upon teachers sending students to the library to use the Internet:

> Some teachers send children to the library to use the Internet and so on. Year 11 are doing project work, so they're able to use the computers. They have a task and its expected that they will have made some progress with that task. Well in a way, that's surveillance isn't it. You might not have somebody

looking at you but they are expecting some results (Mary, Head of IT, Eastway).

Mary noted that the teachers who sent students out of class to work in the library might not be able to observe their on-line activity, but since the students were expected to do a set amount of work this in effect acted as a form of surveillance. At Greenswold, I talked to several students who were studying for General National Vocational Qualifications. These students related how they were allowed to leave the classroom to use the Internet for assignment work which they later had to show to the teachers. While checking the amount of work done by a student might give some indication as to their activities, it is far from an effective method of surveillance. Indeed three male students who had been sent out of the classroom to use the Internet in the Learning Resource Centre at Forestfields, were observed quickly finishing their tasks, before indulging in recreational "surfing" for computer games sites. When the end of the lesson approached the students briefly discussed whether they should return to the class five or ten minutes before the end of the lesson.

During the research period, none of the five secondary schools had CCTV cameras inside the buildings. However, towards the end of the fieldwork Forestfields was considering bids for the installation of cameras in the Learning Resource Centre. Liz the librarian at Forestfields explained that "the cameras are really just to see if we knew something happened, we could perhaps scan the tapes. But really we don't have very much damage or vandalism" (Liz, librarian, Forestfields). According to Liz, the primary motivation for installing CCTV was to focus on vandalism and students stealing books rather than Internet misuse. Nevertheless, CCTV would enable staff to monitor which students used computers at particular times. Such positive identification could be useful in situations where students challenge the evidence of computer website logs by suggesting that someone else has used their Internet password to access unsuitable sites.

Overall, in secondary schools physical surveillance was carried out by staff who focused on computer screens, printed material and work completed. Students also

watched each other's on-line activities, although only Forestfields set up a formal system where sixth form students became monitors. While limited space dictated that as many Internet machines as practically possible should be situated in ICT rooms, screen visibility was still considered an important factor. Ultimately physical surveillance was largely concerned with curbing the intentional misuse of the school Internet by "dangerous students".

2.3 Post 16-institution

At Hightree Tony, the ICT manager, stated that there was always a member of staff supervising Internet activity. In the main ICT suite, which was adjacent to the library, this task fell to the librarian. Yet during the research the librarian was absent for two months due to illness and nobody took her place. According to the students ICT staff and teachers who passed through the Internet suite often cast an eye over their activities.

Jim, the Head of science at Hightree, argued that the placing of Internet computers had been largely an issue of efficient use of space. Hence, throughout the college computers were positioned in back to back rows. In the main Internet suite, there were twelve computers, on each side of the room, back to back in three groups of four. The computers at each end of the room faced the nearby wall. Students choosing to get up to mischief on-line tended to favour these end computers. Thus when a student attempted to "hack" into the administration account it was one of these end computers that was used. Indeed Ben a year 13 student noted that if he wanted to go on prohibited chat-lines "its easier if you're at the bottom two or those corner two, because it's difficult to see the screens" (Ben, tear 13 Hightree). Once more, this illustrates that some students were aware of the importance of screen visibility.

Tony remarked that in addition to looking at computer screens he also observed general student behaviour. He explained:

> We look for the clues such as groups gathering round. That's usually groups of lads gathering round. So you can listen for animated, excited conversation,

> listen to the noise levels rising and then intervene (Tony, ICT manager, Hightree).

Thus, Tony argued that while he might not always be able to see the computer screens he could watch general student behaviour and interpret signs of excited chatter as an indication that they might be misusing the Internet. In a sense, Tony relied on student reactions to notify him of unsuitable on-line activities.

At Hightree, cameras had been installed in the library after a spate of book thefts. Yet, Tony also noted the cameras could be seen as part of a policy of surveillance that was concerned with student Internet use.

> Interviewer: Was there any consideration of using CCTV to monitor PC and Internet use?
> Tony: Yes. This one [points to camera] has a view to the opposite corner. So really that only addresses the stations which are facing this way. But it wasn't really to see an image of what's on the screen, it was about the general behaviour, if they were gathering.

Tony notes that using CCTV cameras did not actually allow him to see on-screen Internet images. Rather the cameras enabled him to keep an eye on general student behaviour. He also argued that recorded material could be potentially useful in identifying who used a machine at a particular time.

2.4 Summary

In both primary schools while staff watched student on-line activity, viewing computers screens and printed output, they argued that they were concerned with students accidentally rather than intentionally accessing unsuitable material. This suggested that physical surveillance in the primary schools potentially served the purpose of safeguarding "students-at-risk" from on-line hazards. In contrast physical surveillance in the post-primary schools was largely concerned with restricting intentional misuse of the Internet by the "dangerous student".

3. Virtual surveillance of "net" activity

Physical surveillance focusing on students behaviour, computer screens, printed material, CCTV images and work done enabled staff to follow student on-line activity. Furthermore, an array of computer mediated observation tools also existed. These "virtual surveillance" applications enabled staff to either reconstruct the on-line wanderings of a student or view the screen of any networked terminal. The two main devices available for virtual surveillance of student activities were programs that logged the addresses of websites visited and software, such as "Net-top teacher", which allowed staff to view and control any computer in a networked system. Before describing the fieldwork schools' use of virtual surveillance, I shall consider these applications in more detail.

Whenever individuals use the Internet, they render themselves detectable. As Selwyn notes:

> By logging onto a website, by participating in an on-line discussion group and by running a query through a search engine, any individual is inevitably leaving an electronic trail far more permanent and conspicuous than the ephemerality of cyberspace would suggest (Selwyn, 2000: 249).

The profiling and registering of Internet users through so-called "cookies" is commonplace (Lyon, 2001). Such Client-Side Persistent Information devices attach themselves to "surfers", log the websites visited and download this information upon returning to their "home site". These devices tend to be used by commercial organisations seeking to build up consumer profiles of the "net" users who visit their websites. Yet, on-line activities are not just logged by devices in cyberspace, the computers used to access the Internet also carry much information about an individual's on-line activities. Thus with a few clicks of the mouse, a recent history of websites visited or the stored list of documents downloaded from the web can be accessed. Staff can also examine student computer accounts to see if they have stored any unsuitable material on the school computer hard drive. Furthermore, many schools use specialist software that records, in a central database or "log", the on-line addresses of all the websites accessed. As students often have to sign onto the Internet using an

individual password, it is possible for staff not only to identify the websites visited but also which student accessed the site. As some of the website addresses contain an indication of the nature of their content staff can identify which students have visited unsuitable websites. If there is uncertainty about the nature of a particular website then staff can access the address and experience first hand the material that the student saw. Insofar as these computer logs provide comprehensive records of the websites visited by Internet users, they contain an immense amount of information.

In addition to specialist software that records the addresses of websites visited, certain applications, such as Net Top Teacher, allow staff to view networked computer screens and control the activities of these machines. Net Top Teacher is software aimed at enhancing the teaching process. Thus, from a master computer teachers can view students' screens to ensure they are following instructions correctly and take control of the computer to correct certain actions when the student has made a mistake. However, insofar as staff can use this software to covertly observe students on screen activity and where necessary seize control of computers, Net Top Teacher also provides an effective surveillance tool. Indeed the ability to control other networked computers means that staff can potentially expose on screen windows that students may have minimised or hidden behind other material.

In considering the use of virtual surveillance applications in the fieldwork schools I will focus in turn upon the primary, secondary and post-16 institutions.

3.1 Primary schools

Both Avenue and Brooklands primary schools had access to computer logs that recorded the addresses of websites visited by students. However, according to staff at these schools there had been no reason to examine these logs. Discussing these computer logs of websites visited Ella, the ICT co-ordinator at Avenue, explained, "we have them, but we haven't had call to use them ... the students behave themselves" (Ella, ICT co-ordinator, Avenue). While Ella noted that the school had no recourse to refer to the computer logs, she inferred that only in a

situation where students misbehaved on-line would the need arise. A similar view was expressed by Cliff the Head of Brooklands, who argued that "we don't look at logs. But I they're always there just in case we need to check whether one of the children have been looking at, shall we say, unsuitable material" (Cliff, Head, Brooklands). Thus, Cliff affirmed the potential usefulness of computer logs where staff thought that a student has accessed unsuitable material. In a sense, Cliff suggested that such virtual surveillance was likely to take place after an incident occurred. However, staff at both schools were adamant that no incident had given them recourse to use the computer logs to reconstruct the on-line wanderings of a student.

While neither school had Net Top Teacher, Avenue had software that enabled students from different networked institutions to work collaboratively on a single computer screen. However, Ella noted that the software was a purely educational tool, which they had only experimented with a few times. Of course, such software has potential as a surveillance tool, but the description of this item by Ella purely in terms of educational benefits indicated a lack of concern with virtual surveillance.

Despite possessing applications that would allow the schools to carry out virtual surveillance of student on-line activity, neither Avenue nor Brooklands made use of these facilities. Arguably, this situation could be explained by noting that virtual surveillance is primarily concerned with monitoring the activities of the "dangerous student". Ella the ICT co-ordinator at Avenue argued that students behaved, so there was no requirement to examine the computer logs of websites visited. Insofar as Internet risk in primary schools were seen in terms of the "student-at-risk" there was no apparent need to carry out virtual surveillance of the activities of the "dangerous student". Hence, virtual surveillance systems, able to observe the on-line activities of students, remained unused.

3.2 Secondary schools

All the secondary schools in the research had some form of virtual surveillance application which allowed staff to check which websites had been visited by students and examine material that had been downloaded from the web.

At Canalside, Wilf the Head of IT used computer logs of websites visited to identify which students had visited adult chat-lines using the school Internet. He was able to identify students by their Internet user names and track their on-line activities. However, he found it difficult to hold students accountable for their "surfing" activities, merely by using the computer logs as students reportedly often claimed that somebody else had used their password. Staff at Dalehouse were able to block a pornographic website constructed on a student's home computer after they had examined computer logs to check the on-line address. At Eastway, the ICT technicians used the computer logs to reconstruct the on-line activities of the students who "hacked" into the school network. On one occasion when ICT staff were using the computer logs they noted that an on-line student had a "hacking" program open. While Mary the Head of IT went to the library and physically watched the activities of the student in question the technicians followed his on-line actions. Kate the ICT co-ordinator at Forestfields explained how the technician occasionally "trawled" through student accounts and website logs to ensure that they hadn't accessed unsuitable on-line material. She also noted that when students had been caught accessing pornography the computer logs had been used as evidence in deciding the punishment. Robert, the ICT manager at Greenswold related that "on a Friday night we go through and have a look at the logs and just have a look at what JPEG's they have" (Robert, ICT manager, Greenswold). Thus Robert not only skimmed through the addresses of websites visited by students, but paid attention to any material downloaded from the web, specifically graphic files, so-called JPEG's.

The ICT manager at Greenswold noted there was a major drawback with the comprehensiveness of computer logs. He observed that "in principle these logs exist, but in practice you finish up with a hard drive full of logs and nobody has got any time to read them anyway" (Robert, ICT manager, Greenswold). Beth, a

business studies teacher at Greenswold, highlighted a further weakness of computer logging systems, complaining that some pornographic websites had innocuous titles and web addresses that concealed their true nature. Thus, she told how she had stumbled across a website with the innocent web address of bankaccount.com, which turned out to be a pornographic site. This use of innocuous on-line addresses makes it difficult to identify the nature of some websites accessed by students.

IT literate staff in the secondary schools were aware of the existence of specialist programs, such as Net Top Teacher, which allowed remote access to a student's computer. However during the research period Greenswold was the only secondary school that possessed such software. Net Top Teacher, as the name suggests, had been designed as a teaching aid, enabling staff from a central terminal to take control of a student's workstation and show them how to execute procedures. With regards to surveillance, programs such as Net Top Teacher allowed staff to remotely close windows on screen, click on icons and see if students were attempting to hide anything within the screen. As the ICT manager at Greenswold noted:

> We've got Net Top Teacher. You can control everybody's computer, from one computer. So, you can always see what kids have got on screen. You can actually get into their computer screen and open windows they're trying to hide. That might be very good, but when you've got thirty [students] in a room, it's certainly difficult (Robert, ICT manager, Greenswold).

Robert noted the potential benefits of Net Top Teacher as a virtual surveillance tool, namely, the ability to see what students had on screen and access material that they were attempting to conceal. However, as Robert suggested observing as many as thirty screens in a classroom situation could prove difficult. Despite the existence of the Net Top teacher software in the school Robert was unable to provide an example of a situation where it had been used as either an educational or surveillance tool.

Some evidence suggested that the various methods of virtual surveillance gave rise to a degree of panopticism. For example, at Forestfields a year eight student

discussing the degree of surveillance of student Internet use, argued that "if you go on the Internet all the time Mr Smith [name changed] the head he like checks it on the server. So he knows which one you've been on" (Kenny, year 8, Forestfields). Kenny fearing that the Head constantly checked student Internet activity, avoided using the Internet for excessive periods of time and thereby carried out a degree of self-policing. Certainly, the computer logs were checked, although Kate the ICT co-ordinator denied that the Head carried out this task. While interviewing John, a year 13 student at Forestfields, I mentioned the idea that the Head checked all the on-line activities of students. He replied "he doesn't, but he can. It's the threat of knowing that he can. It logs all the history of what you've been looking at" (John, year 13, Forestfields). I would argue that the potential threat, mentioned by John, that staff could observe all on-line activity gives rise to a degree of self-surveillance.

Overall, all secondary schools in the research used computer logs and data on material downloaded from the "net" to carry out virtual surveillance of on-line activity. While some of this surveillance was in response to particular incidents of misuse, there was also a tendency for staff to "trawl" computer logs to see if students had accessed unsuitable websites. At all five secondary schools following incidents of student Internet misuse staff used computer logs in an attempt to reconstruct events. Such activities can be seen as focusing upon the on-line actions of the "dangerous student". Virtual surveillance in secondary schools can be seen as an attempt to make students accountable for Internet misuse. While one secondary school in the research had Net Top Teacher there was no evidence to suggest that it was used either in a educational or surveillance capacity.

3.3 Post-16 institution

Tony the ICT manager at Hightree explained how he had used computer logs to provide evidence that a student had accessed a particular website that contained pornographic material. In this case, a member of staff had physically observed the student's activities so the information drawn from the computer logs merely acted as supporting evidence. Additionally Tony noted how he had also used the

computer logs when he had grown concerned about the inordinate length of time some students seemed to be spending on the college Internet.

> I started to go through the logs and the logs are absolutely enormous. Every single movement is recorded in the logs. So I piled all the data into a spreadsheet and laid it out and had a look at it. I found names that were cropping up 8.30 in the morning. They might go on and off a little bit, but they were basically there towards the end of the day. So, we started challenging these people (Tony, ICT manager, Hightree).

Thus, the computer logs enabled Tony to observe how long particular students were on the college Internet. With the evidence from these logs, staff were then able to confront students who made excessive use of the Internet and encourage them to focus on off-line college work. According to Tony, the task of analysing the data was difficult due to the sheer size of the logs, which recorded every single on-line movement.

Hightree did not make use of any applications such as Net Top Teacher. However, Alan an English teacher at the college remarked that the school attended by his son used this software, as they were "paranoid" about students misusing the Internet. He noted that Hightree College would be unlikely to adopt such a package, as it would require an increase in staffing to be used effectively.

3.4 Summary

While virtual surveillance applications existed in the primary schools, they were not used. However, in the secondary and post-16 institutions involved in the research student on-line activity was monitored through the use of software that logged the addresses of websites visited and the material downloaded from the web. This was done to reconstruct incidents of Internet misuse and to speculatively check whether students were abusing the school network. While this meant that virtual surveillance often occurred after an incident, there were situations in which such observation took place while a student was misbehaving. For example at Eastway ICT technicians were able to follow a student's on-line activities while he used a "hacking" program. Furthermore, programs such as Net Top Teacher potentially allowed staff to view networked computer screens from

a central machine. While Avenue primary school and Greenswold secondary school had such devices there was no evidence of them utilising this software for surveillance purposes. Computer logs and records were used in the post-primary institutions to hold accountable and punish "dangerous students" for their intentional misuse of the Internet. At Hightree computer logs were also used to identify students who needed to be encouraged to spend less time on-line.

Conclusion

While in the primary schools surveillance served the purpose of protecting the "student-at-risk" from the effects of accidentally accessing unsuitable on-line material, in post-primary schools observation was concerned with curtailing intentional Internet misuse by "dangerous students" and making them accountable for their actions. Thus in secondary and post-16 institutions surveillance potentially nurtured accountability, sought to reinforce social order and through the effects of panopticism introduced an element of self-policing.

Three considerations were central to understanding the nature of physical surveillance, namely, the identity of the observer, the focus of the observation and the use of space. It was noted that in primary, secondary and post-16 institutions a range of staff including teachers, ICT specialists, librarians, and lunchtime support staff were involved in monitoring on-line use. Additionally there existed an element of peer surveillance, with students observing one another's activities. While the importance of screen visibility was recognised in schools, in the post-primary schools the pressure to fit a large number of networked machines into a room tended to mean that surveillance issues were secondary to spatial efficiency. Nevertheless, staff recognised the importance of being able to see students' computer screens to monitor their on-line activities. Additionally staff observed printed output from the web, CCTV screens and the amount of work done. While in primary schools physical surveillance of Internet use was related to the need to protect children at risk from on-line hazards in secondary and post-16 institutions such activities served the primary purpose of protecting the school from the "dangerous student".

Schools carried out virtual surveillance by examining the computer logs of websites accessed by students and checking the items downloaded from the web. Although two schools in the research owned educational software that effectively allowed staff to spy on students' on-screen activity there was no evidence that such applications were actually used for this purpose. In primary schools staff acknowledged that computer logs of the websites visited by students existed but stated that they had not actually used them. This lack of use was explained in terms of the good behaviour of students on-line. Arguably, this also reflected the lack of concern in primary schools about the potential threat of intentional Internet misuse by the "dangerous student". In secondary and post-16 institutions, computer logs were used to reconstruct incidents of Internet misuse, keep checks that students were not accessing unsuitable websites and to provide evidence of misuse in an attempt to make students accountable for their on-line actions. In this sense, virtual surveillance in post-primary schools was concerned with curtailing the activities of "dangerous students" and holding them accountable for Internet misuse.

Having considered school attempts to control Internet use and deal with issues of risk, in this and the previous two chapters, in the final chapter I summarise the arguments and evidence that I have presented. Thus I shall consider the conclusions of this research, reflect upon the research process, outline the main implications of my findings and suggest future avenues for research.

Part Five

Conclusion

In chapter twelve I draw together my research findings, outline the implications of these findings, reflect on the research process and indicate some possible areas for future research.

Chapter Twelve

Conclusion

Introduction

Drawing upon fieldwork in eight educational institutions this research has explored the risks arising from school Internet use. Thus, in the previous sections of this thesis I have considered the research background, described the staff / student Internet risk narratives, assessed whether the risks discussed were actual or perceived and outlined the schools' attempts to control Internet use. In drawing this thesis to a conclusion I will review the main findings of the research as presented in the preceding chapters. I shall then focus on the main implications of my research, both for school Internet use and the sociology of risk literature, before reflecting on the research process. Finally, I will suggest some possible directions for future research.

1. Summary of research findings

In summarising my research findings I will focus in turn on staff / student risk perceptions, the assessment of school Internet risks and the attempts by educational institutions to control Internet use.

1.1 Staff / student perceptions of risks arising from school Internet use

When exploring risk narratives from a cultural perspective there is a need to reflexively examine the viewpoints of the various social actors (Douglas, 1985, 1992: Wynne 1989, 1996), such as the staff and students in the case of school Internet use.

Of the thirty staff interviewed across the eight educational institutions. twenty-eight expressed concern about pornography, twenty-four about chat-lines, three focused on hate engendering sites, two were worried about websites promoting experimentation, seven considered the legal threat arising from copyright

violation and nine discussed the dangers posed to network security. In discussing their concern, staff drew variously upon the narratives of the "student-at-risk" and the "dangerous student". The "student-at-risk" can be perceived as being physically or mentally in danger from the on-line activities of paedophiles, or the accidental accessing of illegal and harmful material on the net. Arguably this is in contrast to the "dangerous student", who poses a risk to others' reputation, security or finances through his / her on-line activities.

The majority of staff interviewed saw pornography and chat-lines as problems. Although the concern about on-line pornography related mainly to the threat to school image in post-primary schools, concerns for students using chat-lines was more balanced between the "student-at-risk" / "dangerous student" narratives. While copyright violation was a concern for some teachers, students tended only to be described as creating a risk insofar as they downloaded pirated music files onto the school system. Network security issues were couched almost entirely in terms of the "dangerous student". Few staff raised the issue of hate engendering sites or websites encouraging experimentation with explosives or drugs. Overall with regard to hazards arising from the Internet primary school staff tended to perceive their students as being "at risk". This was in contrast to the post-16 institution where staff saw students' misuse of the Internet largely as a source of danger to staff and the college. In secondary schools these narratives were much more intertwined with Internet activity being viewed variously as putting students at risk and creating danger for the schools.

While concern was expressed in staff interviews about the dangers arising from school Internet use, one of the most notable features of the student risk narrative was its almost non-existence on a verbal level. Although sixty three students were asked about the problems and dangers that they felt arose from school Internet use very few expressed concerns beyond the problems of web searches producing too many hits, the pitch of websites and the reliability of on-line information. Indeed at four institutions students did not express any concern about on-line dangers. This response can be seen as reflecting a genuine lack of anxiety amongst students about on-line hazards. Eleven students discussed the problem of on-line pornography, though only two of these expressed concern that

they might accidentally stumble across such material while using the school Internet. Although the majority of students interviewed touched upon the subject of chat-lines only five students labelled them as "risky". One of these students explained that while he had been harassed on-line he simply asked the cyber-chat provider to block certain messages. Three students expressed concern about security issues relating to the school Internet, but only one of these was directly worried about the threat to the school network posed by "hackers".

Reflecting on staff and student risk narratives it should be noted that categories such as the pornographic, hate engendering or dangerously experimental were not always easy to define. Furthermore, it was not always obvious whether schools were likely to face prosecution for copyright violation. This is not to deny that many cases emerged where a consensus existed but rather to suggest that there were some borderline areas where interpretation was problematic. Diverse perspectives could and in some cases did lead to differential labelling of the same material. Drawing upon the influence of various writings on postmodernity Lawson and Comber (2000a) maintain that the introduction of the Internet into schools has the potential to blur certain boundaries, confusing existing categories. Thus the World Wide Web allows for the removal or distortion of a host of referential signs which individuals use in assessing the legitimacy or suitability of material (Lawson and Comber, 2000a). For example, images of nudity that might be tacitly tolerated in magazine form may become redefined as unsuitable or even pornographic when accessed on-line. While some students discussed competing perspectives over what might be seen as pornographic material on-line, there was evidence that they understood that teachers' definitions mattered when it came to school Internet use and the possibility of punishment. Indeed the impact of the social world in imposing frames of reference is somewhat underplayed by Lawson and Comber (2000a). As Adam and Green (1998) and Joo (1999) note the influence of existing boundaries in the wider socio-economic world still provide a strong determinate of on-line activity. Finally it can be argued that certain material, such as propaganda or hate sites, might be reconstructed as appropriate educational resources if resituated in a structured learning environment.

1.2 Assessing staff / student risk perceptions of school Internet use

When assessing whether certain Internet risks are actually a threat to student, staff or school a distinction needs to be made between actual and perceived risks. Actual risks can be seen as having an existence in the physical world insofar as they or comparable hazards have been realised. Perceived risks can be described as purely imagined dangers where anticipated or comparable hazards exist only in discourse in the social world. For a risk to be labelled as actual a judgement needs to be made as to whether someone has suffered as a consequence of the same or a similar risk coming to pass.

Pornography is widely available on the Internet (Malamuth and Impett, 2001), diverse in it's nature (Myers, 1996: Akdeniz, 1997) and frequently accessed in wider society (Tarpley, 2001). Aware of such factors the educational institutions involved in this research had controls in place to restrict accidental or intentional access to such material in school. In this context I argued that two issues needed to be considered when focusing on the subject of students viewing on-line pornography in school, the number of students exposed to such material and the effect of the exposure. While some students in all post-primary schools in the research saw on-line pornography via the school Internet, such incidents seem to have been rare. Psychological research tends to be concerned with the influence on children of long-term exposure to pornography (Donnerstein and Smith, 2001). Students were not subjected to such prolonged exposure in the schools studied. In this context, I argued that occasional, brief viewing of such material had little apparent affect on students. In summary, I argued that the psychological risk to students posed by occasional, brief exposure to pornography on-line was perceived rather than actual.

Cases of adults seducing young children over the Internet have occurred in wider society (Telegraph, 25.10.00). While, no such incidents were reported in any of the schools studied, two girls did consider meeting up with strangers they chatted to on-line and a student visited a girl whom he had previously only communicated with via the web. There was no evidence in primary institutions of children using chat-lines in school. Overall, given that incidents have occurred

where children have been seduced on-line and then physically abused in the real world, I accepted that the risks offered by chat-lines were actual ones. However, drawing upon the lack of such Internet related incidents in schools I maintained that such risks were statistically remote.

The increasing use of the Internet by extremists to promote hateful attitudes and actions against ethnic, religious and same-sex orientated groups is a cause for concern (Whine 1997: Kallen, 1998). The possibility that impressionable children might access such websites is worrying. While racist material has long existed off-line, putting such material on the World Wide Web increases students' chances of stumbling across it. However, I note that during the whole of my fieldwork in eight educational institutions only one incident of students accessing a racist website was reported. While hate engendering websites offered an actual risk, especially to young children who might accept such hateful views without question, the reportedly rare incidence of students accessing such sites led me to conclude that this risk was statistically remote. Yet it should be noted that the known existence of such sites might have a general negative effect on minority groups, making them feel threatened.

As Wallace and Mangan (1997) note there is nothing new about bomb or drug making recipes on the Internet. Despite two staff expressing concern about such experimentation sites only one incident was reported. In this case the website, which described cannabis use, was deemed to be educational by the ICT manager at the school. As experimentation with dangerous narcotic or explosive materials might result in physical harm, I would not deny that websites featuring "recipes" promoting drug or bomb making are an actual risk. Yet, students did not appear to be attracted to such on-line material.

While there were no reported incidents of students "flaming" dignitaries using e-mail with the school identity attached, there were cases in all-post primary schools studied of students intentionally accessing pornographic material and having sexual on-line chats using the school Internet. Despite these incidents no school was singled out for negative media attention. Insofar as incidents of such Internet misuse are not rare, I argued the media focus was more likely to be on

the general phenomenon rather than individual incidents. There was no evidence of parental complaint relating to this issue in the schools studied. I concluded that the risk to the institutional image arising from students misusing the Internet to "flame" dignitaries, access pornography or engage in on-line sex chats was perceived rather than actual. Additionally, on the positive side, the school Internet could be used as an effective marketing device (Hesketh and Selwyn, 1999). Indeed several of the fieldsite schools had already set up websites with a view to marketing their institution.

The issue of whether the "dangerous student" using the school Internet challenged staff authority was a difficult one to assess. This was because it was tied up with wider issues of power and control in classrooms. In the research, staff concerns about this risk had been muted possibly reflecting that a challenge to their authority was not a new issue. While I noted that the Internet did pose a risk to staff authority I concluded that it should be seen as the extension of the existing problem of power in schools. Furthermore I argued that the Internet might pose a challenge to the teacher's traditional role as the "expert", while maintaining that teachers could avoid such problems by not using the Internet in school.

Copyright is a complex problem for schools, insofar as it is not obvious when or even whether legal action will be taken. Certainly in all the schools studied there was evidence of staff and students infringing copyright. Additionally in three post-primary institutions there was evidence of students downloading MP3 music files onto the school system. During the period of research none of the schools studied were the subject of legal action due to copyright violation. Indeed, in the primary schools staff who were interviewed explained that they understood that as long as they did not profit from copyright violation they would not be prosecuted. In conclusion, I argued that legal action against the schools arising from student copyright infringement was a perceived risk. Even where companies did take action against students downloading pirated music, such as against the University of Oregon, the institution was encouraged to resolve the problem itself (Times Educational supplement, 11.02.00).

Finally, I argued the activities of the "dangerous student" that threatened system security, such as stealing passwords and attempting to "hack" into the school network, could be seen as actual risks. Indeed in seven of the eight schools students gained access to the Internet using someone else's password. With the increasing availability of free pre-designed "hacking" software on the web this problem is likely to worsen (Times, 11.01.01).

It should be noted that while the concept of the "dangerous student" was useful in analysing school Internet use in secondary and post-16 institutions it was not appropriate for students in the primary schools studied. After all, despite one incident of a student using his older sister's password to gain entry to the "net", students appeared to pose little risk to school image, staff authority or security.

1.3 Controlling school Internet use

Lawson and Comber (2000b) note that educational institutions seek to control Internet use through restricting access to Internet machines, utilising filtering software, adopting Acceptable Use Policies, undertaking virtual surveillance and encouraging the use of an honour system. While such policies were evident in my fieldsite schools, they formed part of what could be seen as a broader approach to Internet control that utilised institutional rhetoric, exclusion and surveillance.

Focusing upon the use of institutional rhetoric as an instrument of Internet control I argued that institutions attempted to construct discursively what constituted inappropriate Internet use through verbal communication, Acceptable Use Policies, visual aids such as posters and third party pressure from students' parents. While verbal communication, AUPs, visual aids and third party pressure were primarily used in post-primary schools to protect against "dangerous students", in primary schools verbal communication was used to warn the "student-at-risk" about on-line dangers.

Staff sought to exclude the source of Internet risks in all the schools in the research. Thus, dangerous material or individuals outside the schools were

excluded, while students who intentionally misused the Internet were expelled from the Internet, ICT rooms or ultimately the school.

Schools used a variety of software such as "deny lists" and keyword-matching software to exclude unsuitable on-line material. Additionally two post-primary institutions used a graphic content management application that blocked images with large amounts of skin tone. Students were also excluded from accessing school Internet machines through certain actions. Rooms were locked, passwords used and networks disabled to restrict student access to the Internet. In all post-primary schools in the research students were ejected from machines for accessing unsuitable websites. Furthermore, in four of the secondary schools students were prohibited from using the school Internet for a period of time following incidents in which they had intentionally accessed on-line pornography. In the post-16 college a student was expelled for accessing a website that was deemed by staff to be pornographic. While in primary schools exclusion policies were primarily concerned with protecting students, in the secondary schools safeguarding the institution was also a concern. Indeed, in the post-16 institution excluding material and students were used primarily to protect the college from the on-line activities of the "dangerous student".

A precedent for recognising surveillance as a form of control can be found in the writings of Selwyn (2000) on the National Grid for Learning, Foucault (1977) on panopticism and Ball (2000) on the use of surveillance cameras. While Selwyn (2000) highlights the surveillance capacity of on-line technology, he largely ignores the role of the schools themselves in carrying out both physical and virtual surveillance of staff and students. Rather he focuses on the potential of the NGfL to act as a central conduit for school based performance data, website registration information and electronic trails of site users (Selwyn, 2000: 248-9). Yet in the fieldsite schools there was no evident concern with the surveillance activities of external bodies, rather surveillance was primarily undertaken by staff and focused upon student activity. Drawing on Foucault (1977) and Ball (2000) I argued that surveillance of school Internet could be seen as a form of control, insofar as it was an attempt to impose social order and accountability.

Considering issues of observation and control three issues were central to understanding physical surveillance, namely, the identity of the observer, the focus of observation and the use of space. I noted that in primary, secondary and post-16 institutions a range of staff including teachers, ICT specialists, librarians, and lunchtime support staff were included in the process of monitoring. Additionally there existed an element of peer surveillance, with students observing one another's on-line activities. While the importance of screen visibility was recognised in schools, in the post-primary institutions economic pressures to fit a large number of networked machines into a room meant that surveillance issues were secondary to spatial efficiency. Staff also monitored printed output from the web, CCTV screens and the amount of work done. Schools carried out virtual surveillance by examining the computer logs of websites accessed by students and checking the items downloaded from the web.

Although a couple of schools in the research owned educational software which effectively allowed staff to spy on a student's on screen activity there was no evidence that such applications were actually used for this purpose. While I argued that in the primary schools surveillance served the purpose of protecting the "student-at-risk" from the effects of accidentally accessing unsuitable on-line material, in post-primary schools observation was concerned with curtailing intentional Internet misuse by "dangerous students" and making them accountable for their actions. Thus in secondary and post-16 institutions surveillance was aimed at nurturing accountability, reinforcing social order, introducing an element of self-policing and reconstructing incidents of misuse.

2. Implications of the research for school Internet use

Drawn from the research findings this thesis has four main implications for school Internet use. Firstly, it illustrates that staff need to ask who is at risk when considering school Internet use. Secondly, it suggests that given current controls staff should not be overly concerned about the dangers of students accessing pornographic material via the school Internet. Thirdly, it suggests that while schools need to be aware of copyright issues and inform their students about relevant laws in the current legal climate they are unlikely to be prosecuted for

copyright violation. Finally, I argue that educational institutions need to be made more aware of the threat to network security. Students should be informed that "hacking" into the school network is a serious offence and confidential information should be stored on closed networks that students cannot access. I will now consider these implications in more detail.

Moran-Ellis and Cooper (2000) note that government literature says little about children and technology beyond the conventional construction of children as learners and future adults. Rather an unproblematic picture is painted of the relationship between the Internet and schools, in which the technology is presented as benign (Moran-Ellis and Cooper, 2000: para 2.4). Yet my research indicates that staff, and to a lesser extent students, perceive school Internet use as posing risks. If such on-line dangers are to be understood and avoided then people should be encouraged to ask the question *who is at risk?* In educational institutions, posing this question would allow staff and students to clarify their concerns while making it easier for them to take appropriate action. Moran-Ellis and Cooper make the valid point that "if the Internet is identified as posing risks (in adult terms) to children ... [the] ... educational nature of the Internet becomes unstable" (Moran-Ellis and Cooper, 2000: para 2.4). Yet it should be noted that children using the Internet can also be a source of risk. The categories of the "student-at-risk" and "dangerous student" emerged from both the fieldwork and reflection on Oswell's (1998) article on children and on-line content. I argued that these two categories were not necessarily exclusive, but rather that at various times the student could be at risk and / or dangerous. Furthermore, I maintained that the relative chance of one or other of these labels being applied was age related. While Oswell's (1998) discussion is aimed primarily at academics, practitioners should be made aware of the need to identify the potential victims of risk. Indeed encouraging staff to ask whether their concern about Internet use focuses on the "student-at-risk" or "dangerous student" will allow them to move away from general concerns, such as on-line pornography, and concentrate specifically on the nature of the feared outcomes. Such a focus will potentially allow staff to be more effective in dealing with on-line danger. After all the actions that schools take to protect students on-line may well be different from that to protect their own reputation.

Lawson and Comber (2000b) note that media attention on school Internet use tends to be focused upon the dangers of young people gaining access to pornographic material. While they label these concerns as an example of "moral panic", insofar as they can be seen as exaggerated and sensationalistic, they nevertheless recognise that schools are still likely to be battlegrounds between those seeking censorship and those opposing it. Yet this research indicates that with the Internet controls already in place staff need not be overly alarmed about students accessing pornography or chat-lines via the school Internet. In all six post-primary institutions some students accessed pornographic material and engaged in unsuitable on-line conversations. These events were dealt with as any other incidents of misbehaviour would be in school. Indeed, at Greenswold secondary school the ICT manager compared students accessing pornography on the school Internet to bringing pornographic magazines into school. In this sense, the problems created by Internet use were not seen as being radically different from existing ones. While incidents did occur, they were reportedly uncommon and no evidence suggested that the feared outcomes, of children suffering psychologically or the damaging of institutional reputations, came to pass. While concern amongst psychologists about exposure to pornographic material focuses on heavy viewing over a long period of time (Donnerstein and Smith, 2001) none of the reported cases in the schools studied were described as examples of prolonged exposure. This is not to suggest that on-line pornography itself is not a problematic issue but rather that the current controls that schools operate ensure that teachers should not be overly worried about students accessing pornographic material via the school Internet.

While a wide range of copyright infringements occurred in the schools involved in the research no prosecutions resulted. Of course, this issue might change if commercial organisations choose to enforce their ownership of copyright. While I would not seek to offer legal advice this situation currently indicates that companies are reluctant to prosecute schools for copyright infringement as long as the schools do not profit from such an act. In both of the primary schools in the research staff were well informed about this situation and used material subject to copyright to enhance the learning process where appropriate. In the secondary and post-16 institutions staff were concerned with students

downloading pirated MP3 music files onto the school network. While staff who worked with the Internet were generally aware of issues of legal liability relating to pirated music, students were largely ignorant about this issue. To redress this situation schools should seek to inform students about the legal implications of copyright violation, particularly with regard to MP3 music, using posters or Acceptable Use Policies.

Finally, I would argue that attention should be focused on the issue of on-line security. In wider society "hacking" costs large corporations billions of dollars each month. Increasingly teenage e-vandals use freely available, readymade hacking codes to cause mayhem on-line (Times, 11.01.01). Thus students seeking to hack into the school network do not require expert programming knowledge but rather a website address from where they can download these "hacking" devices. According to the IT Head at Eastway students who hacked into the school network used just such a readymade device. Schools need to inform students about the seriousness of attempts to "hack" into the institution's network. This point is made in light of staff comments that they felt students didn't appreciate that "hacking" was a serious school offence. Following the "hacking" incident at Eastway, a long paragraph about the serious legal consequences of such actions was included in the Acceptable Use Policy. Additionally staff need to be aware of the security issues relating to their own local area networks. If administration information such as staff reviews, reports or even salary information is stored on-line, staff need to be able to ensure the integrity of the local network from internal as well as external "hackers". From a practical viewpoint I would suggest that schools should avoid putting confidential information on networks which, are accessible to students. Rather confidential information should be stored on closed, separate networks accessible only to members of staff.

3. Research implications for the sociology of risk

Reflecting upon the research process and a critical engagement with writings on risk, I argue that this thesis makes three main contributions to the sociology of risk literature. Firstly, if risk is to be comprehensively understood as part of both

the natural and social worlds, analysis should include not only risk narratives and an assessment of the actual dangers but also a description of attempts to control risks. Secondly, within this broad approach, risk narratives need to be considered from a hermeneutic perspective. For reasons I will discuss below this hermeneutic understanding should arise from both interviews and observation within the "risk environment". Finally, in assessing risks there is a need to move the focus away from risk processes to include consideration of risk outcomes. I will now consider each of these main points in turn.

To fully understand risk from a sociological perspective I would argue that it is necessary to focus on risk narratives, risk assessment and attempts to alleviate danger. I would maintain that to ignore any of these aspects would result in an incomplete picture of a particular domain of risk.

While an important insight is offered by risk perspectives which focus on the ways in which the discourses, strategies, practices and institutions around a phenomenon such as risk bring it into being and serve to construct it (Lupton. 1999: 84), to exclude a consideration of actual danger is somewhat limited. Both Foucauldian approaches and elements of Mary Douglas's work have been criticised for reducing real dangers to little more than metaphor, trivialising actual risks and "eliminating danger altogether" (Kaprow, 1985; 347). There is a need to assess danger that threatens people in the social, psychological and physical worlds. Individuals need an analysis of risk that helps inform them of where dangers actually lie so that if they wish and are able to they can take appropriate action. As Wynne (1996) notes, natural scientists and politicians are central figures in risk assessment and education. Yet, it might be argued that there is a role for sociology in identifying actual risks and suggesting different alleviation strategies.

If risks pose serious dangers there is a need not only to understand the nature of such hazards but also to analyse the attempts to alleviate this risk. It might appear to be somewhat ambitious to call for a sociological approach involving a description of risk narratives, an assessment of danger and an analysis of attempts to control risks, yet if social research is to meet wider social needs then

this must be done. If this thesis had concentrated exclusively on staff / student risk narratives then it would have been a somewhat limited piece of work. With such a limited focus I could have said nothing about the actual on-line dangers or the attempts by the school to control school Internet use. Considering the degree of moral panic (Akdeniz, 1997: Lawson and Comber, 2000b) which surrounds the issue of children using the Internet there is certainly a strong argument for making a risk assessment of the on-line dangers.

Furthermore, as concluded in this research actual dangers threaten students, staff and the educational institutions. To ignore the very real threat of issues such as on-line paedophiles, racist websites or compromises to network security would have been negligent, ignoring issues that were of concern both in schools and wider society. Reliable knowledge of on-line dangers can assist staff in dealing with risks arising from the school Internet use. Additionally, a description of school attempts to control Internet use and thereby alleviate risk offers insights into possible risk control instruments while highlighting some pitfalls involved in their use.

In summary sociological research into risks should include an analysis of risk narratives, an assessment of actual dangers and a description of attempts at control. This allows for a comprehensive understanding of a particular danger, while providing a range of information that could help in risk avoidance. Within this broad approach, I would further argue that risk narratives need to be understood from a hermeneutic perspective and that risk assessments should focus on outcomes not just processes. These two issues will now be considered in turn.

It is necessary to adopt a hermeneutic perspective when considering risk narratives so that a comprehensive, situated understanding of the cultural and social aspects of risk can emerge. The early writings on risk of Beck and Giddens' have been criticised for largely ignoring such social and cultural aspects of risk. (Lash, 1994; Day, 2000). Indeed in initial writings both Beck and Giddens largely ignored the importance of non-expert apprehensions and lay-responses to expert systems, rather leaning towards a strongly realist viewpoint.

Such approaches fail to consider the risk perceptions of lay people, often presenting expert knowledge as being synonymous with rational risk perceptions. To fully understand risk perceptions there is a need to move away from this focus on the viewpoint of experts. However, this bias should not be replaced by the privileging of lay person knowledge, for this would merely invert the existing scientific knowledge hierarchies (Szerszynski et al, 1996: 7). Rather risk narratives need to be interpreted and understood from a hermeneutic perspective. Thus, it is necessary to understand risk narratives as they exist within the wider world-view of both experts and lay people. Importantly I argue that it is difficult to get a hermeneutic appreciation of risk merely through interviewing social agents. Rather I maintain that to gain access to world-views that are alien to the researcher observation is also required.

Insofar as social actors may not be fully aware of their own motivations or actions a hermeneutic understanding needs to come not just from interviews but also from observation of "risk behaviour" and the "risk environment". Indeed such observation can also act as a check to ensure that interviewees are not misleading the researcher. In this research, had I merely interviewed students about their Internet risk perceptions then the data collected would have indicated that there was little expressed concern. However, I also carried out observation of students' school Internet use. As discussed in chapter four, students were observed engaging in a wide range of activities that could be viewed as attempts to avoid staff surveillance and subsequent punishment. For example students hid monitor screens, adjusted consoles so they could not easily be seen by observers, chose Internet machines in secluded corners, hid web pages behind other work, used other students passwords and waited for unsupervised "windows of opportunity" to misuse the Internet. While I argue that such activities could not strictly be seen as risk avoidance, I nevertheless maintain that any understanding of the student risk narrative would have been limited without an awareness of this anxiety.

In assessing risks, a distinction should be made between the process and outcome. Both "risk society" approaches, which rely heavily on rhetoric (Lupton, 1999) and cultural perspectives, tend to present an unproblematic relation

between risk processes and outcomes. However, drawing on models used in the social policy analysis (Klein, 1989) it can be argued that a risk is part of a complex social process, where an activity or occurrence (input) leads to an experience (process) which has an immediate result (output) and longer term effects (outcome). For example, with reference to the analysis of on-line danger, web based chat-lines could be seen as a risk input. Students finding such material may engage in conversations (processes) with immediate responses, excitement, revulsion or fear (output). In the longer term students may be subjected to actual physical harm if they meet up with and are abused by strangers (outcome). Attempts to reduce risk occurrence tend to focus on inputs and processes, whereas any concern with the effects of a risk relates to outputs and outcomes.

Research into risks needs to move away from discussing environmental or health risks in simplistic general terms instead identifying a risk process, and then developing the examination by focussing on the feared risk outcome. For example, racist websites can be seen as risk inputs or processes, the feared risk outcomes are the possible consequences that accessing such material might have on individuals and institutions. In this research, there is a constant attempt to develop the analysis beyond simplistic descriptions of risk process and focus on potential risk outcomes. Thus in chapter three while I describe the concern of twenty-eight staff with on-line pornography I subsequently establish the nature of the outcomes that the staff actually fear. While staff were anxious about the process of students accessing on-line pornography, the risk outcomes that worried them were the possible psychological effects on students and the damage to the school reputation. Any research into risk needs to take into account not only the risk process but also the feared risk outcomes.

In conclusion, if risks are to be comprehensively understood sociological research needs to focus not only on risk narratives and risk assessment but also on attempts to control dangers. Furthermore, within this broad approach, risk narratives need to be understood from a hermeneutic perspective and risk assessments should focus on outcomes rather than processes. Having considered the contributions of this research to the sociology of risk literature, I will now

briefly reflect upon what I might do differently if I was to begin this research process again.

4. Reflections on the research

Contemplating my research over the last three years I will now briefly discuss some issues which with hindsight I might now approach differently. Thus I will briefly consider the evolutionary nature of the research process, those individuals omitted from the interview process, the dynamic nature of risk perceptions and the neglect of the "staff-at-risk" / "dangerous staff" narratives. Additionally I will highlight some issues that were omitted from the final version.

While the evolutionary research approach I adopted generated much information, the initial broad focus meant that I spent time and effort gathering information that later proved irrelevant. Indeed, I recognise that if I had constructed a more clearly defined research focus when starting my study I would have made more efficient use of my time and energy. Of course having an emergent focus also had its advantages, as I was able to hone my research skills and gather a range of information that I can use for articles in the future. Additionally because of the sensitive nature of some of the topics I covered it is possible my initial broader focus resulted in schools being more open to the research than they otherwise might have been.

When seeking to interview individuals about school Internet use I recognised that certain groups would be difficult to include in this research process, such as students banned from the Internet, senior managers and parents. Thus only upon one occasion was I able to interview a student punished for serious misuse of the Internet. I believe that it would have been informative to interview students who had been temporarily banned from the Internet or expelled from school because of their on-line activity. There was also little research data gathered from managers in post-primary schools and no governors were interviewed during the research. This was partly a reflection of the limit of time and my desire to interview as large a number of staff and students as possible. Neither were any parents interviewed, although some staff did talk about their own children's

experiences of the Internet. By focusing on staff and students, I was able to achieve an adequate cross section of these two groups but, as I have noted, this invariably resulted in a relative neglect of other possible interviewees.

While I attempted to gather information on the *changing* staff / student views of school Internet risk I recognised that my efforts in this particular area were somewhat limited. Thus while I interviewed the staff with the main responsibility for Internet provision in each of the eight schools twice I was not able to interview the majority of teachers or students a second time. I would argue that to reliably assess changes in the risk narratives a longer time frame would be necessary. Indeed I believe it would be informative to study school Internet risks a few years after the completion of the NGfL to assess whether there had been a change in attitudes and risks.

One area of the research that was neglected was the degree to which staff were at risk and / or a source of danger. Rather I focused largely on risks to the students and the institutions. Nevertheless, I touched upon the subject of inappropriate Internet use by staff (chapter four) and briefly considered how the student might threaten staff authority through their Internet activity (chapter eight). I felt justified in only discussing these issues in passing as, reflecting the social situation in schools, my research generated little relevant information on this area

During the research a large amount of data was collected that was omitted from the final thesis because it related to issues which I perceived to be of secondary importance. Thus, a section discussing writings on moral panic and research data linking this phenomenon to staff attitudes about on-line risks was cut from the final thesis. Information relating to "effective" Internet use, the playing of on-line games and barriers to educational gains was left out because I felt these issues did not relate directly to risk (this issue is further discussed in chapter three). Information on gender and differential Internet use was gathered but as I believed this data offered few useful insights I decided that this would be better as a future focus of research. Finally, I omitted a section on the simulation of surveillance from my final draft. This was because, despite some interesting work on

surveillance and simulation (e.g. Bogard, 1996), I felt there was little evidence of the use of simulation as an instrument of school Internet control.

Overall I believe the research methods I used were effective in gathering data which enabled me to understand, interpret, analyse and evaluate risks arising from school Internet use. Having reflected upon my research, I will now consider possible directions for future research related to both school Internet use and the sociology of risk.

5. Future directions for research

In briefly reflecting upon possible future areas for research into Internet use and risk I will touch upon gender, identity and alternative locations of on-line provision.

While there has been much written about computer use and gender, there is currently little that examines the issue of how Internet use differs between genders. Although I was not able to reach any firm conclusions in my research about gender differences regarding Internet use and risk some of the information gathered hinted at interesting possibilities. For example, males were responsible for all the reported incidents of students intentionally accessing pornographic images. On the other hand staff such as the ICT manager at the post-16 college argued that more female than male students used the college Internet to engage in sexual on-line chats. Both male and female students were mentioned in staff discussions about issues of authority, security and copyright. I would argue that any gender differences in school Internet use do not have any implications for the main arguments put forward in this thesis. Yet I would also maintain that the issue of gender and Internet use might provide an interesting area for future research.

Another question of interest that emerged from the research was whether students intentionally misused the Internet to create risk and thereby forge an aspect of their identity. Lupton (1999) notes that there is a tendency for some people to engage in risky activities not only for pleasure, but also as an important element

of identity construction. The extent to which students engaged in "hacking" or downloading pornographic material were actively trying to construct their identity as a "risk takers" might prove an interesting area for research. Indeed, the ICT Manager at the post-16 institution related how one girl argued that using chat-lines in school was a "rite of passage". This begs the broader question of whether students used the school Internet to construct personal identity and / or redefine themselves.

Finally, while my research was located in schools I would suggest that there are other locations that deserve attention. Thus, little is known about Internet use and risk in domestic houses, public libraries, community centres, Internet cafés and networked offices. I would argue that all these areas provide potential areas for research.

Conclusion

In this chapter, I have drawn together the main findings of my research into the risks arising from school Internet use. Thus, I have reviewed the differing risk perceptions of staff and students, the evaluation of these risks and the institutional attempts to control Internet use. Additionally I highlighted the implications of this research both for school Internet use and the sociology of risk literature. Finally, I reflected upon the research process and suggesting future avenues of enquiry. I now will briefly recap on the main implications of this research.

With regards to school Internet use I argued that there were four elements of my research findings that might have important implications. Firstly, staff need to ask who is at risk when considering school Internet use. Considering both the "student-at-risk" and "dangerous student" narratives will enable them to clarify their concerns and take appropriate action. Secondly, while incidents of students accessing pornography or engaged in sexual on-line "chats" did occur in all the post-primary schools studied, no evidence suggested that psychological or reputation damage resulted. Thirdly, although a wide range of copyright infringements occurred in the schools involved in the research no prosecutions

resulted. This situation suggests that companies are reluctant to prosecute schools for copyright infringement as long as the schools do not profit from such an act. Finally, attention should be focused on the issue of on-line security. If administration information such as staff reviews, reports or even salary information is stored on-line, staff need to be able to ensure the integrity of the local network from internal student "hackers".

Reflecting upon sociological writings on risk, I argued that this thesis made three main contributions to the sociology of risk literature. Firstly, it illustrated that if risk is to be comprehensively understood, analysis needs to include not only risk narratives and an assessment of the actual dangers but also a description of attempts to control risks. Secondly, within this broad approach, this research showed that risk narratives need to be considered from a hermeneutic perspective. Finally, in assessing risks I argued that there is a need to move the focus away from risk processes to include consideration of risk outcomes.

As Jones (1998) notes the history of the Internet is still being written. Over thirty years since the creation of the Internet and ten years since the construction of the World Wide Web social commentators are still attempting to assess the impact of this new technology. Within this context, my research is an attempt both to develop the sociology of risk through a multi-site case study in one area of social life and to clarify some of the risks related to this developing technology and its use in schools. Whether the nature of these on-line risks will change over time is a matter for future consideration and as such is well beyond the remit of this current research.

Bibliography

Adam, A. & Green, E. (1998) Gender, agency, location and the new information society, in B. D. Loader, (ed.) *Cyberspace Divide: Equality, Agency and Policy in the Information Society*. London: Routledge. pp. 83-97

Akdeniz, Y. (1997) The Regulation of Pornography and Child Pornography on the Internet, *The Journal of Information, Law and Technology (JILT)* <http://elj.warwick.ac.uk/jilt/internet/97_1akdeniz.html>

Ball, M. (2000) The Visual Availability and Local Organisations of Public Surveillance Systems: The Promotion of Social Order in Public Spaces, *Sociological Research On-line*, Vol. 5, No. 1, <http://www.socresonline.org.uk/5/1/ball.html>

Bauman, Z. (1993) *Postmodern Ethics*. Oxford: Blackwell.

Baym, N.K. (1998) The Emergence of On-line Community, in S. G. Jones, (ed.) *Cybersociety 2.0 Revisiting Computer-Mediated Communication and Community*. London: Sage. pp. 35-68.

BBC News On-line (09.04.98) Teachers' fear over Internet porn <http://news6.thdo.bbc.co.uk/hi/english/uk/newsid_76000/76184.stm>

BBC News On-line (10.10.99) Net porn warning for pupils <http://news.bbc.co.uk/hi/english/education/newsid_470000/470299.stm>

BBC News On-line (11.10.99) Safety net warning against porn <http://news.bbc.co.uk/hi/english/education/newsid_469000/469550.stm>

BBC News On-line (07.11.01) Pupils expelled over Internet ecstasy <http://news.bbc.co.uk/hi/english/uk/scotland/newsid_1642000/1642646.stm>

Beck, U. (1992) *Risk Society: Towards a New Modernity*. London: Sage.

Beck, U. (1994) The reinvention of politics: towards a theory of reflexive modernization, in U. Beck, A. Giddens, & S. Lash (eds) *Reflexive Modernization, Politics, Tradition and Aesthetics in the Modern Social Order*. Cambridge: Polity Press. pp. 1-55.

Beck, U. (1995) *Ecological Politics in the Age of Risk*. Cambridge: Polity Press.

Beck, U. (1996a) World risk society as cosmopolitan society? Ecological questions in a framework of manufactured uncertainties. *Theory, Culture and Society*, 13(4), pp.1-32.

Beck, U. (1996b) Risk society and the provident state, in S. Lash, B. Szerszinski, and B. Wynne (eds) *Risk, Environment and Modernity: Towards a New Ecology*. London: Sage. pp. 27-43.

Beck, U. and Beck-Gernsheim, E. (1995) *The Normal Chaos of Love*. Cambridge: Polity Press.

BECTa (1996) *Managing IT in Primary Schools: a planning tool for senior managers*. Coventry: BECTa.

BECTa (1997a) *The Internet and the World Wide Web*. Coventry: BECTa.

BECTa (1997b) *Censorship Issues and Filtering Software*. Coventry: BECTa.

BECTa (1997c) *Security and Ethics*. Coventry: BECTa.

BECTa (1998) *Connecting Schools, Networking people: ICT Planning Purchasing and Good Practice for the National Grid for Learning*. Coventry: BECTa.

Bell, D. (1976) *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. Harmondsworth: Penguin.

Berkowitz, L, & Rogers, K. H. (1986) A priming effect analysis of media influences, in J. Bryant and D. Zillmann (eds) *Perspectives on Media effects* Hillsdale, NJ: Lawrence Erlbaum. pp. 57-82.

Blunkett, D. (1997) On the starting grid, *Educational Computing and Technology*, December 1997, pp. 11-12.

Bogard, W. (1996) *The Simulation of Surveillance.* Cambridge: Cambridge University Press.

Bradbury, J. (1989) The policy implications of differing concepts of risk, *Science Technology & Human Values*, 14(4), 380-399.

Bryant, J. (1985) Frequency of exposure, age of initial exposure and reactions to initial exposure to pornography, in D. Zillmann & J. Bryant (eds) *Pornography: Research advances and policy considerations.* Hillsdale, NJ: Lawrence Erlbaum. pp. 183-196.

Bujra, J. (2000) Risk and Trust: Unsafe sex, gender and AIDS in Tanzania, in P. Caplan (ed.) *Risk Revisited.* London: Pluto Press. pp 59-84.

Caplan. P. (2000) Introduction: Risk revisited, in P. Caplan (ed.) *Risk Revisited.* London: Pluto Press. pp 1-28.

Carter, D. (1997) 'Digital democracy' or 'information aristocracy': Economic regeneration and the information economy, in B. D. Loader (ed.) *The Governance of Cyberspace: Politics, Technology and Global Restructuring.* London: Routledge. pp. 136-152.

Castel, R. (1991) From dangerousness to risk, in G. Burchell, C. Gordon and P. Miller (eds) *The Foucault Effect: Studies in Governmentality.* London: Harvester / Wheatsheaf. pp. 281-98.

Castells, M. (1996) *The Information Age: Economy, Society and Culture. Volume I: The Rise of Network Society.* Oxford: Basil Blackwell.

Castells, M. (1998) *The Information Age: Economy, Society and Culture. Volume III: End of Millennium.* Oxford: Basil Blackwell.

Conservative Party (1997) *Election Manifesto.* London: Conservative Party.

Danet, B (1998) Text as Mask: Gender, Play and Performance on the Internet, in S. G. Jones (ed.) *Cybersociety 2.0 Revisiting Computer-Mediated Communication and Community.* London: Sage. pp. 129-158.

Day, S. (2000) The Politics of Risk among London Prostitutes, in P. Caplan (ed.) *Risk Revisited.* London: Pluto Press. pp 29-58.

Dean, M (1999) Risk, calculable and incalculable, in D. Lupton (ed.) *Risk and Sociocultural Theory: New Directions and Perspectives.* Cambridge: Cambridge University Press. pp. 205-28.

Denning, D.E. (1997) The future of cryptography, in B. D. Loader (ed.) (1997) *The Governance of Cyberspace: Politics, Technology and Global Restructuring.* London: Routledge. pp 175-189.

Denzin, N.K. (1989) *Interpretative Interactionism.* London: Sage.

DfEE (1997a) *Connecting the Learning Society.* London: Stationary Office.

DfEE (1997b) *Preparing for the Information Age: Synoptic Report on the Evaluation of the Education Departments' Superhighways Initiative.* Suffolk: DfEE.

DfEE (1999) *Superhighway safety: Safe use of the Internet.* Sudbury, Suffolk: DfEE.

Dietrich, D. (1997) (Re)-fashioning the Techno-Erotic-Woman: Gender and Textuality in the Cybercultural Matrix, in S.G. Jones (ed.) *Virtual Culture: Identity & Communication in Cybersociety*. London: Sage. pp. 169-184.

Donnerstein, E. and Smith, S. (2001) Sex in the Media, in D. G. Singer & J. L. Singer (eds) *Handbook of Children and the Media*. London: Sage Publications. pp. 289-307.

Douglas, M. (1985) *Risk Acceptability According to the Social Sciences*. New York: Russell Sage Foundation.

Douglas, M. (1992) *Risk and Blame: Essays in Cultural Theory*. London: Routledge.

Douglas, M. and Wildavsky, A. (1982) *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Berkley, California: University of California Press.

Downey, J. (1999) XS 4 All? 'Information Society' Policy and Practice in the European Union, in J. Downey & J. McGuigan (eds) *Technocities*. London: Sage. pp. 121-138.

Elgesen, D. (1996) Privacy, Respect for Persons and Risk, in C. Ess (ed.) *Philosophical Perspectives on Computer-Mediated Communication*. New York: State University of New York Press. pp. 45-66.

Ess, C. (1996) Introduction: Thoughts along the I-way; Philosophy and the Emergence of Computer-Mediated Communication, in C. Ess (ed.) *Philosophical Perspectives on Computer-Mediated Communication*. New York: State University of New York Press. pp. 1-14.

European Commission (1996a) *Green Paper on the Protection of minors and human Dignity in Audiovisual and Information Services,* Com (96) 483 Final, Brussels, 16 October.

European Commission (1996b) Communication from the Commission to the European Parliament, the Economic and Social Committee and the Committee of the Regions on *Illegal and Harmful Content on the Internet*, Com (96) 487, Final, Brussels, 16 October.

European Parliament (1999) Action Plan on Promoting Safer Use of the Internet, Decision No. 276 / 1999/ EC of the European Parliament and the Council. *Adopting a Multinational Community Action Plan for promoting safer use of the Internet by combating illegal and harmful content on global networks*, 25 January 1999.

Firestone, W. A. & Herriot, R. E. (1984) Multisite qualitative policy research: some design and implementation issues, in D. M. Fetterman (ed.) *Ethnography in Educational Evaluation.* Beverley Hills, CA: Sage. pp. 63-88.

Foster, P. (1996) *Observing Schools: A Methodological Guide.* London: Paul Chapman Publishing.

Foster, D. (1997) Community and Identity in the Electronic Village, in M. Porter (ed.) *Internet Culture.* London: Routledge. pp. 23-37.

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison.* London: Allen Lane.

Foucault, M. (1991) Govermentality, in G. Burchell, C. Gordon and P. Miller (eds) *The Foucault Effect: Studies in Governmentality.* London: Harvester / Wheatsheaf. pp. 87-104.

Frissen, P. (1997) The virtual state: Postmodernisation, informatisation and public administration, in D. Loader (ed) *The Governance of cyberspace: Politics Technology and Global Restructuring.* London: Routledge. pp. 111-125.

Furedi, F (1997) *Culture of Fear: Risk Taking and the Morality of Low Expectation.* London: Cassell.

Furlong, A. & Cartmel, F. (1997) Growing up in the risk society, *Sociology Review*, 7(2), pp. 27-30.

Furlong, J., Furlong, R., Facer, K. & Sutherland, R. (2000) The National Grid for Learning: a curriculum without walls? *Cambridge Journal of Education*, Vol. 30, No.1, 91-110.

Gerbner, G., Gross, L., Morgan, M. and Signorielli, N. (1994) Growing up with television: The cultivation perspective, in J. Bryant & D. Zillmann (eds) *Media Effects*. Hillsdale, NJ: Lawrence Erlbaum. pp. 17-41.

Giddens, A. (1991) *Modernity and Self-Identity*. Cambridge: Polity Press.

Giddens, A. (1994) Living in a post-traditional society, in U. Beck, A. Giddens & S. Lash (eds) *Reflexive Modernization, Politics, Tradition and Aesthetics in the Modern Social Order*. Cambridge: Polity Press. pp. 56-109.

Giddens, A. (1998) Risk society: The context of British politics, in J. Franklin, (ed.) *The Politics of Risk Society*. Cambridge: Polity Press. pp. 23-34.

Glaser, B. & Strauss, A. (1967) *The discovery of grounded theory*. Chicago: Aldine.

Greco, M. (1993) Psychosomatic subjects and the "duty to be well": Personal agency within medical rationality. *Economy and Society*, 22(3) pp. 357-72

Gross, J. (04.05.01) Personal correspondence from Walt Disney Company (Europe): Unpublished

Hammersley, M. (1980) On interactionist empiricism, in P. Woods (ed.) *Pupil Strategies*. London: Croom Helm. pp. 67-83.

Hammersley, M. (1992) *What's wrong with Ethnography?* London: Longman.

Hammersley, M. (1998) (2nd Edn.) *Reading Ethnographic Research.* London: Longman.

Hammersley, M. & Atkinson, P. (1995) *Ethnography: Principles in Practice.* London: Routledge.

Handwerker, L. (1994) Medical risk: Implicating poor pregnant women, *Social Science and Medicine*, 38(5) pp. 665-75.

Haywood, T. (1998) Global networks and the myth of equality: trickle down or trickle away? in B. D. Loader (ed.) *Cyberspace Divide: Equality, Agency and Policy in the Information Society.* London: Routledge. pp. 19-34.

Hesketh, A. J. & Selwyn, N. (1999) Surfing to School: the electronic reconstruction of institutional identities. *Oxford Review of Education*, Vol. 25, No. 4, 501-520.

Holderness, M. (1998) Who are the world's information-poor? in B. D. Loader (ed.) *Cyberspace Divide: Equality, Agency and Policy in the Information Society.* London: Routledge. pp. 35-56

Institute for Historical Review (1995) *Update,* February 1995, Institute for historical Review: California

Independent (15.02.01) When just looking is no excuse

Jaunch, M. (1998) Policing the Internet in NCH Action for Children, *Children on the Internet: Opportunities and Hazards.* London: NCH Action for children. pp. 15-17.

Jones, S.G. (1998) Information, Internet and Community: Notes towards an Understanding of Community in the Information Age, in S. G. Jones (ed.) *Cybersociety 2.0 Revisiting Computer-Mediated Communication and Community.* London: Sage. pp. 1-34.

Joo, J. (1999) Cultural Issues of the Internet in Classrooms, *British Journal of Educational Technology*, Vol. 30, No. 3, 245-250.

Kahn-Egan, C. N. (1998) Pandora's boxes: Children's reactions to and understanding of television and Internet, rules, ratings and Regulation. Unpublished: Florida State University.

Kallen, E. (1998) Hate on the Net: A Question of Rights / A Question of Power. *Electronic Journal of Sociology*: 3, 2. <http://www.lycoming.edu/library/symposium/hate.htm>

Kaprow, M. (1985) Manufacturing danger: fear and pollution in industrial society, *American Anthropology*, 87, pp. 342-356.

Keen, J., Ferguson, B., and Mason, J. (1998) The Internet, other "nets" and healthcare, in B. D. Loader (ed.) *Cyberspace Divide: Equality, Agency and Policy in the Information Society*. London: Routledge. pp. 217-235.

Kellner, D. (1999) New Technologies: Technocities and the Prospects for Democratisation, in J. Downey & J. McGuigan, (eds) *Technocities*. London: Sage. pp. 186-204.

Kennedy, M. M. (1979) Generalizing from single case studies, *Evaluation Quarterly*, 3 (4). pp. 661-78.

Klein, (1989) *The Politics of the NHS*. London: Longman.

Kumar, K. (1995) *From Post-Industrial to Post-Modern Society*. Oxford: Basil: Blackwell.

Labour Party, (1997) *Election Manifesto*. London: Labour Party.

Lash, S. (1994) Reflexivity and its doubles: structure, aesthetics, community, in U. Beck, A. Giddens & S. Lash (eds) *Reflexive Modernization, Politics,*

Tradition and Aesthetics in the Modern Social Order. Cambridge: Polity Press. pp. 110-73.

Lawson, T. and Garrod, J. (1996) *The complete A-Z sociology handbook.* London: Hodder & Stoughton.

Lawson, T. and Comber, C. (2000a) Introducing Information and Communications Technologies into Schools: the blurring of boundaries. *British Journal of Sociology of Education* 21 (3) pp. 419-433.

Lawson, T. and Comber, C. (2000b) Censorship, the Internet and Schools: a new moral panic? *The Curriculum Journal* 11 (2) pp. 273-285.

Lecker, S. (1985) *Improvised Explosives: How to make your own*. New York: Paladin Press.

Lofland, J.& Lofland L.H. (1995) *Analyzing Social Settings: A guide to Qualitative Observation and Analysis*. Belmont, California: Wadsworth.

Lupton, D. (1999) *Risk*. London: Routledge

Lyon, D. (2001) *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.

MacRae, S. (1997) Flesh Made Word: Sex, Text and the Virtual Body, in M. Porter (ed.) *Internet Culture*. London: Routledge. pp. 73-86.

McLaughlin, M. L., Osborne, K. K. and Ellison, N. B. (1997)Virtual Community in a Telepresence Environment, in S. G. Jones (ed.) *Virtual Culture: Identity & Communication in Cybersociety*. London: Sage. pp. 146-168.

Malamuth, N. (1996) Sexually explicit media, gender differences, and evolutionary theory, *Journal of Communication*, 46 (3), pp. 8-31

Malamuth, N. & Impett, E. (2001) Research on sex in the Media: What Do We Know About Effects on Children and Adolescents? in D.G. Singer & J. L. Singer (eds) *Handbook of Children and the Media.* London: Sage Publications. pp. 269-287

Markus, T. A. (1993) *Buildings and Power.* London: Routledge.

Mead, D. (1998) An overview of the implications of the Internet for child welfare, in NCH Action for Children, *Children on the Internet: Opportunities and Hazards.* London: NCH Action for children. pp. 6-8.

Mitra, A. (1997) Virtual commonality: Looking for India on the Internet, in S.G. Jones (ed.) *Virtual Culture: Identity & Communication in Cybersociety.* London: Sage. pp. 55-79.

Morais, R.C. (1999) Porn goes public, *Forbes Magazine.* June 14, 1999. p.214.

Moran-Ellis, J. and Cooper, G. (2000) Making Connections: Children, Technology, and the National Grid for Learning. *Sociological Research On-line*, vol. 5, no. 3 <http;//www.socresonline.org.uk/5/3/moran-ellis.html>

Moschovitis, C. J. P., Poole, H., Schuyler, T. and Senft, T.M. (1999*) History of the Internet: A Chronology, 1843 to the Present.* Santa Barbara, California: ABC-Clio.

Myers, W. (1996) Fun.nl - Live sex on the Internet, *Wired UK*, 1996, 2.10, pp. 50-56.

Negroponte, N. (1995) *Being Digital.* London: Hodder & Stoughton.

OFTEL (1997) *Information Highways: Improving access for schools and colleges and public access points.* London: OFTEL.

Oswell, D. (1998) The place of "childhood" in Internet content regulation: a case study of policy in the UK, *International Journal of Cultural Studies*, 1, 131-151.

Plant, S. (1996) On the Matrix: Cyberfeminist Simulations, in R. Shields (ed.) *Cultures of Internet: Virtual Spaces, Real Histories, Living Bodies.* London: Sage. pp. 170-183.

Poster, M. (1990) *The Mode of Information: Post-Structuralism and Social Context.* Cambridge: Polity Press

Poster, M. (1997) Cyberdemocracy: Internet and the Public Sphere, in M. Porter (ed.) *Internet Culture.* London: Routledge. pp. 201-217.
Poster, M. (1998) Virtual Ethnicity: Tribal Identity in an Age of Global Communications, in S. G. Jones (ed.) *Cybersociety 2.0 Revisiting Computer-Mediated Communication and Community.* London: Sage. pp. 184-211.

Powell, W. (1970) *The Anarchist Cookbook.* New York: Barricade Books.

Resnick, P. and Miller, J. (1996) *PICS: Internet access without censorship* <http://www.w3.org/PICS/iacwcv2.htm>

Rheingold, H. (1994) *The Virtual Community.* London: Secker & Warburg.

Robson, (1993) *Real World Research: A resource for Social Scientists and Practitioner-Researchers.* London; Blackwell.

Rose, N. (1985) *The Psychological Complex.* London: RKP.

Russell, G. & Russell, N. (1999) Cyberspace and School Education, *Westminster Studies in Education*, Vol. 22, 7-17.

SCET (1996) *Information Ethics: creating an ethical and safe environment.* Glasgow: SCET.

Schofield, J.W. (1993) Increasing the generalizability of qualitative research in M. Hammersley (ed.) *Educational Research: Current issues, volume one.* London: Paul Chapman Publishing. pp. 91-113.

Schofield-Clark, L. (1998) Dating on the Net: Teens and the Rise of "Pure" Relationships, in S. G. Jones (ed) *Cybersociety 2.0 Revisiting Computer-Mediated Communication and Community.* London: Sage. pp 159-183.

Selwyn, N. (1997) Assessing Students' Ability to Use Computers: theoretical considerations for practical research, British Educational Research Journal, Vol. 23, No. 1, 47-59.

Selwyn, N. (1999a) The Discursive Construction of the National Grid for Learning, *Oxford Review of Education*, Vol. 26, No, 1, 63-79.

Selwyn, N. (1999b) Gilding the Grid? The marketing of the national grid for learning, *British Journal of Sociology of Education*, 20, 1, pp. 59-72.
Selwyn, N. (1999c) Why the Computer is not Dominating Schools: a failure of policy or a failure of practice? *Cambridge Journal of Education*, Vol, 29, No. 1, 77-91.

Selwyn, N. (2000) The National Grid for Learning: panacea or Panopticon? *British Journal of Sociology of Education,* Vol. 21, No. 2, 243-255.

Shaw, D.F. (1997) Gay Men and Computer Communication: A Discourse of sex and Identity in Cyberspace, in S. G. Jones (ed.) *Virtual Culture: Identity & Communication in Cybersociety.* London: Sage. pp 133-145.

Skelton, C. (1994) Network of Hate: The Dark Side of Cyberspace, *id Magazine,* 3, 2, pp. 9-12.

Spradley, J.P. (1980) *Participant Observation*. New York: Holt, Rinehart & Winston.

Steele, J. (1997) *Information for Citizenship in Europe*. London: Policy Studies Institute.

Stodghill, R. (1998) Where'd you learn that? *Time*, June 15, pp. 52-59.

Strauss, A. & Corbin, J. (1990) *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. London: Sage.

Sunday People (18.10.98) Teenage students rapped over school porn network.

Sunday Telegraph (03.12.00) Paedophiles calling a fifth of children on net.

Szerszynski, B., Lash, S., & Wynne, B. (1996) Introduction: Ecology Realism and the Social Sciences, in S. Lash, B. Szerszinski and B. Wynne (eds) *Risk, Environment and Modernity: Towards a New Ecology*. London: Sage. pp. 1-26.

Tarpley, T. (2001) Children, the Internet and other New Technologies, in D. G. Singer & J. L. Singer (eds) *Handbook of Children and the Media*. London: Sage Publications. pp. 547-556.

Telegraph (23.05.00) Judge demands law change to punish Internet paedophiles.

Telegraph (29.06.00) Porn risk to children.

Telegraph (07.08.00) Children at risk from net fiends.

Telegraph (18.08.00) Six-year-olds may be seeing violence and porn on the net.

Telegraph, (25.10.00) Why the net must be swept clean of paedophiles.

Telegraph (30.03.01) Hacking is now bigger threat than terrorism.

Thomas, D. (2000) New Ways to Break the Law: Cybercrime and the Politics of Hacking, in D. Gauntlett (ed.) *web.studies: Rewiring media studies for the digital age*. London: Arnold. pp. 202-211.

Thomas, D. & Loader, B. (eds) (2000) Cybercrime: Law enforcement, security and surveillance in the information age. London: Routledge.

Thompson, K. (1998) *Moral Panics.* London: Routledge.

Times (16.11.00) The key to cracking down on pornography.

Times (20.11.00) Evil masked by innocence.

Times (11.01.01) Beware of the script kiddies.

Times (13.03.01) Legally indecent?

Times Educational Supplement (14.05.99) Getting a handle on the haters.

Times Educational Supplement (15.10.99) Great leap forward: Not in front of the children.

Times Educational Supplement (11.02.00) MP3 – a sound idea.

Times Educational Supplement (03.03.00) Line drawn between sex and shopping.

Times Educational Supplement (17.03.00) Cyber chat brings teen fantasies to life.

Toffler, A. (1970) *Future shock.* London: Bodley Head

Toffler, A. (1980) *The Third Wave.* London: Collins.

Toffler, A. (1990) *Powershift: Knowledge, Wealth and Violence at the Edge of the 21st Century*. New York: Bantam.

Wallace, J. and Mangam, M. (1997) *Sex, Laws and Cyber-space: Freedom and Censorship on the Frontiers of the Online Revolution.* New York: Henry Holt and Company.

Watson, N. (1997) Why We Argue About Virtual Community: A Case Study of the Phish.Net Community, in S. G. Jones (ed.) *Virtual Culture: Identity & Communication in Cybersociety*. London: Sage. pp. 102-132.

Webster, F. (1995) *Theories of the Information Society.* London: Routledge.

Webster, F. (1999) Information and Communication Technologies: Luddism Revisited, in J. Downey & J. McGuigan (eds) *Technocities*. London: Sage. pp. 60-89.

Whine, M. (1997) The Far Right on the Internet, in B. D. Loader (ed.) *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge. pp. 209-227.

Wilbur, S. P. (1997) An Archaeology of Cyberspace: Virtuality, Community, Identity, in M. Porter (ed.) *Internet Culture*. London: Routledge. pp. 5-22.

Wolcott, H.F. (1994) *Transforming Qualitative Data: Description, Analysis and Interpretation.* Thousand Oaks, California: Sage.

Woods, P. (1979) *The Divided School.* London: Routledge & Kegan Paul

Wynne, B. (1989) Frameworks of rationality in risk management: towards the testing of naïve sociology, in J. Brown (ed.) *Environmental Threats: Perception, Analysis and Management*. London: Bellhaven Press. pp. 33-47.

Wynne, B. (1996) May the sheep safely graze? A reflexive view of the expert-lay-knowledge divide. In S. Lash, B. Szerszinski and B. Wynne (eds) *Risk, Environment and Modernity: Towards a New Ecology*. London: Sage, pp. 44-83.