The following document is from:

Safe and Responsible Use of the Internet: A Guide for Educators

Nancy E. Willard, M.S., J.D.

Responsible Netizen Institute
474 W 29th Avenue
Eugene, Oregon 97405
541-344-9125
541-344-1481 (fax)
Web Site: http://responsiblenetizen.org
E-mail: info@responsiblenetizen.org

Introduction

Overview

The Internet has emerged in the last decade as an extremely important conduit for information and communications. The objective of schools is to prepare students for active and effective participation in society. The information and communication resources of the Internet have become an essential component of this preparation. Schools are uniquely positioned to serve as the primary vehicle through which young people can develop the knowledge, skills, and motivation to use the Internet in a safe, responsible, and effective manner.

Many schools have placed primary reliance on filtering software to address online safety concerns. It has always been recognized that filtering software is imperfect -- it neither blocks all material that should be blocked, and it frequently blocks access to perfectly appropriate material.

There is a growing recognition of the fact that it is simply not possible to protect children with technological tools that are neither infallible, nor present on every Internet access device.

On May 8, 2002, the National Research Council (NRC) released its report entitled *Youth, Pornography and the Internet*[1]. A major conclusion of this report was:

> (S)ocial and educational strategies to develop in minors an ethic of responsible choice and the skills to effectuate these choices and to cope with exposure are foundational to protecting children from negative effects that may result from exposure to inappropriate material or experiences on the Internet.

In the preface to the report, Dick Thornberg, former Attorney General and committee chair, indicated that the report would "disappoint those who expect a technology 'quick fix'" and chided school officials and others for seeking "surrogates to fulfill the responsibilities of training and supervision needed to truly protect children from inappropriate sexual materials on the Internet."

The report noted that much of the focus of attention has been on technology solutions and public policy. "Technology solutions seem to offer quick and inexpensive fixes that allow adult caregivers to believe that the problem has been addressed, and it is tempting to believe that the use of technology can drastically reduce or eliminate the need for human supervision.[2]" But that technology should not be considered an adequate "substitute for education, responsible adult supervision, and ethical Internet use.[3]"

No technology protection measure is or ever will be 100% effective in protecting young people from exposure to material that is potentially harmful. There is simply too much material on the Internet, with more material posted every second, for any technological system to be truly effective. Virtually every young person will, at one time or another, have unsupervised access to the Internet through an unfiltered, unblocked, and unmonitored system. Any time a technology is created that seeks to block access to material, another technology will emerge to get around such blocking actions. Technically proficient young people can easily obtain information on effective strategies to get around these systems.

Schools have become the universal location where young people are learning about the Internet. Certainly, then, schools should have an important obligation to help young people learn to use the Internet in a safe and responsible manner regardless of the presence or absence of any kinds of protective technologies. Schools are also an important conduit of information for parents -- many of whom are not as technically literate as their children.

Interestingly, when the NRC Committee asked educators about the benefit of having filters, in virtually every school the committee visited the primary reasons offered for filters were to avoid controversy in the community and to avoid liability for exposing children to inappropriate

---

[1] National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002) URL: http://bob.nap.edu/html/youth_internet/.

[2] NRC, supra at Section 14.3.

[3] NRC, supra at Section 14.3.

material[4]. Essentially, it appears that the primary reason schools have filters is not to protect kids -- but to protect the school. This is unacceptable.

The most concerning finding in the *NRC Report* is the degree to which young people have had to learn Internet safety skills on their own. As noted:

> Virtually all of the high school students to whom the committee spoke said that their "Internet savvy" came from experience, and they simply learned to cope with certain unpleasant Internet experiences. They also spoke of passing their newfound expertise down to younger siblings, hence becoming the new de facto educators for younger children in the "second wave of digital children[5]."

A recent survey of girls aged 14 to 17 conducted by the Girl Scouts amplifies the reasons for concern[6]. This survey revealed that 30% of girls had been sexually harassed in chat rooms. Yet only 7% of the 30% told an adult about the harassment. Further, the vast majority of girls report that they rely primarily on their own knowledge and skills in dealing with online concerns. *Only 29% of the girls surveyed* reported receiving any Internet safety instruction from teachers. This safety instruction was generally limited to three prohibitive concepts: Don't disclose personal information; Don't talk to strangers; and Don't go to bad sites.

It can be expected that young people are going to have superior technical skills than most adults. But adults are responsible for imparting the knowledge, skills, and values that are essential for young people to learn to make safe and responsible choices.

We, as society, are too often willing to believe that a technological "quick fix" will solve the problem. When we believe in the sufficiency of the technological "quick fix," we fail to engage in the more important actions that are necessary to effectively address the underlying concerns. Far too many decision-makers, educators, and parents believe in a myth -- that the installation and use of a "technology protection measure" will protect children against access to potentially harmful material and people on the Internet. The unfortunate result of the belief in this myth is false security, which leads to complacency, which results in the failure to adequately protect our children by preparing them to use the Internet in a safe and responsible manner.

This is not to say that there is no role for technology tools in the establishment of an environment that supports the safe and responsible use of the Internet by young people. Technology can be used to establish safe spaces for younger students, and to reinforce accountability on the part of older students. The major concern is that a strategy that places primary reliance on technological "quick fixes" will fail to address the far more important issues of education and supervision.

These materials provide guidance for school districts in the development and implementation of a comprehensive education and supervision approach to assist students in gaining the knowledge,

---

[4] See "District Liability Related to Access to Inappropriate Material or People" for a discussion of liability related to access to inappropriate material.
[5] NRC, supra, at Section 14.3.
[6] Whitney, R. (2002) *The Net Effect: Girls and New Media*. Executive Summary. Girl Scout Research Institute, New York. URL: http://www.girlscouts.org/about/PDFs/NetEffects.pdf.

skills, and motivation to use the Internet in a safe and responsible manner. By developing a comprehensive approach to address such concerns, schools can help young people develop effective filtering and blocking systems that will reside in the hardware that sits upon their shoulders.

Core Components of a Comprehensive Approach

Protection and Preparation

The recommendations set forth in these materials are grounded in knowledge of effective parenting and educational strategies. When children are to young to comprehend dangers and make safe choices, we keep them in safe places and closely supervise their activities. We teach them how to recognize and deal with potential dangers – lessons that expand as they grow and face new situations. We also teach them about our positive expectations for their behavior. As children grow, we allow them increased freedom. We do not expect that teens will be willing to remain in fenced play yards. But we also remain engaged – "hands-on" – through ongoing communication and supervision, and, when necessary, appropriate discipline.

These same strategies provide the foundation for a comprehensive approach to address Internet dangers and concerns and the use of the Internet in school.

Focus on the Educational Purpose

Use of the district Internet system should directed to those activities which support education, enrichment, and career development, with the option of limited "open access" times. Districts must support the educational use of the system through professional development, technical and instructional support, Internet-based lesson plans and an educational web site.

The best way to promote the safe and responsible use of the Internet is to ensure that teachers are prepared to lead students on exciting, educationally enriching learning "adventures" on the Internet. When the computers are being used for such activities, the opportunity for misuse is significantly limited.

Education About the Safe and Responsible Use

Teachers, administrators and students should receive instruction related to the safe and responsible use of the Internet. Education for students should be appropriate to their age and understandings. Young people should be empowered to independently handle a wide range of interactions and activities on the Internet that could be harmful to their safety and well-being. Safety concerns include being the target or recipient of sexual predation, hate group recruitment, gaming and gambling, invasion of personal privacy, Internet fraud and scams, harassment, stalking, harmful speech, and access to inappropriate material.

We also must address other issues related to the responsible use of the Internet by young people. In addition to the intentional access of potentially harmful material, these issues include copyright infringement, plagiarism, computer security violations (hacking, spreading viruses), violation of privacy, Internet fraud and scams, harassment, stalking, and dissemination of

harmful speech or other violent or abusive material. We must prepare young people to understand their responsibilities as “cybercitizens.”

Clear Policy that is Well-Communicated

Students and staff should have a clear understanding of the kinds of activities that are and are not considered acceptable. Students and staff should be aware that they have a very limited expectation of privacy when they use the Internet at school. They should have a full and complete understanding of the degree to which their activities will be monitored, how this monitoring will occur, and the circumstances under which a specific investigation of their online activities will occur.

The policy should address access to inappropriate material, the safety and security of students when using electronic communications, unlawful and inappropriate activities, and the protection of student personal information. The policy should address responsibilities of both staff and students.

The policy should serve as the foundation for the district's education program regarding the safe and responsible use of the Internet -- not simply just another document included in the start-of-school informational packet.

Supervision, Monitoring and Appropriate Discipline

Student use of the Internet should be supervised by teachers in a manner that is appropriate for the age of the students and circumstances of use. The type and level of monitoring is somewhat dependent on the circumstances of the school. Supervision and monitoring must be sufficient to establish the expectation that there is a high probability that instances of misuse will be detected and result in disciplinary action. When students are fully aware that there is a high probability that instances of misuse will be detected and result in disciplinary action, they are unlikely to take the risk of engaging in such misuse. The existence of effective monitoring, and student knowledge of such existence is generally sufficient deterrent for misuse.

In small schools with a limited number of students, limited number of computers, and low level of Internet traffic, an approach that involved staff supervision and staff review of Internet records will likely be sufficient to establish the expectation of high probability of detection of misuse. With larger schools, more students, more computers, and a higher level of traffic, supervision and staff review of Internet usage logs will likely not be sufficient to achieve a high probability that instances of misuse will be detected. This is where the use of a technology tool becomes an appropriate consideration. Technology tools allow for the more effective and efficient review of Internet usage and significantly enhances the probability that instances of misuse will be detected.

It is not possible for districts to enforce a wide range of individual family values when students are using the Internet in school. Districts can address parent concerns and support student Internet use in accord with personal family values by allowing parents to have access to their child's Internet use records upon request.

Misuse of the Internet by students should be addressed in a manner that makes use of the "teachable moment" both for the individual student and other students in the school. The focus of such instruction should be on the reasons for the rule -- the issues or concerns regarding the potential harm the rule is designed to address -- rather than a focus on disobedience and the power of the teacher or administrator to impose discipline. No student should ever disciplined for incidents that have occurred that are outside of the control of the student, such as the unintentional access of inappropriate material. No student should ever be disciplined for reporting that they have gotten into a dangerous or concerning online situation.

Children's Internet Protection Act

In December 2000, Congress enacted the Children's Internet Protection Act (CIPA)[7]. CIPA requires that schools and libraries that are seeking certain federal funds for technology certify that they have developed an Internet Safety Plan that meets certain statutory requirements. CIPA also requires districts to install a "technology protection measure" to protect against access to specified inappropriate material.

The approach recommended in this Guide is in accord with the CIPA requirements. However, the primary focus of the materials is on the Internet Safety Plan, not technology protection measures.

Contents of the Guide

This Guide is set forth in four parts:

- Part I addresses the essential components of a comprehensive approach to address the safe and responsible use of the Internet by students.

- Part II addresses the requirements for a Internet Safe and Responsible Use Plan/Policy. This plan follows the requirements contained in the Children's Internet Protection Act (CIPA) for an Internet Safety Plan.

- Part III provides insight into a variety of legal issues that are raised in the context of use of the Internet in school, including district liability, first amendment issues, harmful off-campus speech, copyright, public records and the like.

- Part IV sets forth a variety of documents that can be modified for use by the district, including policy documents, regulations, guidelines, use agreements, and informational materials for parents and community members.

On some occasions, material is repeated in two different locations. For example, supervision and monitoring is both a component of a comprehensive approach and a requirement under the CIPA Internet Safety Plan. Privacy issues are of relevance to the discussion of supervision, and are also an important legal issue. The material is repeated to allow each Part to stand as a "whole." This may be helpful for instructors desiring to use individual Parts for instructional purposes.

[7] 42 U.S.C. 254.

International Readers

Much of this Guide will also be relevant for educators outside of the U.S. Part I sets forth basic strategies that should be relevant in any school environment. Part II is structured in accord with the CIPA Internet Safety Plan requirements, but these requirements are quite general and provide an excellent framework for planning. Part III addresses legal issues and is based solely on U.S. law. Therefore this Part will not be as relevant. Part IV contains materials that should be applicable in any education environment.