Safeguarding the Wired Schoolhouse

A Briefing Paper on School District Options for Providing Access to Appropriate Internet Content

Consortium for School Networking

Acknowledgements

The Consortium for School Networking is a non-profit association that promotes the use of telecommunications to improve K-12 learning. Its members include state departments of education, state networks, school districts, schools, individuals and companies that are committed to this goal.

This project is made possible through the financial support of the corporate sponsors identified below. However, CoSN is responsible for creating all of the materials associated with the project and retains editorial control over them. Sponsors provide input and feedback, but the ultimate responsibility for the project's materials rests with CoSN.

CoSN gratefully acknowledges the support of America Online Inc., Education Networks of America and N2H2 Inc. that made this briefing paper possible. It was prepared by Sara Fitzgerald of Funds For Learning LLC, project director of Safeguarding the Wired Schoolhouse. Additional materials will be made available at the project's Web site, www.safewiredschools.org.

For more information, contact CoSN, 1555 Connecticut Avenue NW, Suite 200, Washington, DC 20036. Phone: 202-466-6296. http://www.cosn.org.

Reuse of This Briefing Paper

A Message from CoSN

Since the mid-1990s, the question of whether Internet content should be screened by Internet service providers, schools and libraries has been the subject of hot debate—within legislative bodies, before the courts and within those organizations themselves.

The Consortium for School Networking has long argued that the decision on whether to manage and monitor Internet usage, and, if so, how best to do it, belongs at the local level. Each school, school district or educational network is best equipped to evaluate its own needs, based on such factors as community norms, the sophistication of its students or users, and its particular computer infrastructure. The "one-size-fits-all" approach advocated by some political leaders fails to acknowledge that not all schools and school districts are alike, and that a solution that may be appropriate for one school district may not be appropriate for the next. Further, CoSN believes that mandating a particular solution will bring to a halt that technological innovation that has been the hallmark of this market since it first emerged a half decade ago.

CoSN launched the "Safeguarding the Wired Schoolhouse" project in the fall of 2000 to help school leaders understand the issues involved in managing Internet content. Its goal is to build on the extensive work that the school community has already done to create positive online experiences for children. The briefing paper hopes to advance that work by helping school leaders understand the technological options that are available to them, and to frame questions that should be considered when making a decision about whether to control their students' access to the Internet.

After CoSN first published this white paper, Congress passed the Children's Internet Protection Act, which requires schools to adopt a technology protection measure to block or filter certain kinds of Internet content as a condition of receiving certain kinds of educational technology funding. The publication of this document should not be read as an endorsement of content controls in general, or a particular technological approach.

CoSN does believe that every school or school district that provides access to the Internet should adopt an Acceptable Use Policy to guide users and system administrators alike. CoSN will continue to work with other educational associations to provide resources to help school officials develop and refine these policies.

Keith Krueger
Executive Director, CoSN

Jim Hirsch
Chair, CoSN
Assistant Superintendent for Technology, Plano ISD, Plano, TX

Executive Summary

As the number of computers in schools and the number of children accessing the Internet from the classroom have grown exponentially over the past few years, so too have the challenges facing educators trying to ensure that children have a positive experience when they go online.

Many earlier initiatives have tried to help parents and teachers understand how to safeguard children when they access the Internet. In addition, many organizations have tried to inform parents about software and other tools that can be used to help protect children going online from a single home computer. But comparatively less attention has been devoted to helping school administrators and teachers understand their specific options, technological or otherwise, for protecting children when they access the Internet over a school-based or statewide educational network.

This briefing paper is designed to address that need by detailing the range of options that are available to schools for managing students' access to the Internet and helping to ensure that their experiences are positive ones.

The briefing paper also provides a list of questions that school officials should consider when deciding whether to manage students' access to the Internet, and, if so, which solution to choose.

No matter which approach a school or school district decides to pursue, it should adopt an Acceptable Use Policy to govern the use of its network and computers. School officials should also take concrete steps to teach their students the "rules of the road" when they go online, and how to evaluate the quality of online information. This briefing paper includes a list of resources that school officials can draw on when they undertake these tasks.

Introduction

Over the past decade, the number of schools with Internet access has grown exponentially, and the number of children going online from school has followed suit. In 1999, the National Center for Education Statistics reported, 95 percent of public schools were connected to the Internet, and, more importantly, 63 percent of public school classrooms had an Internet connection.[1]

Now, some 14 million children access the Internet from school, a figure that is expected to grow to more than 30 million by 2003 as schools continue to build their networks. By that year, it is anticipated that more students will access the Internet from their classrooms than the number who will access it from home.[2]

The Internet truly is like "a vast library including millions of readily available and indexed publications," containing content "as diverse as human thought," as the U.S. Supreme Court described it in a 1997 decision.[3] But just as in any city frequented by millions of people, there are neighborhoods on the Internet that are inappropriate for children to visit alone and strangers they would be better off not meeting.

Throughout the past decade, policy makers, industry advocates, parents and teachers have tried to address these concerns. Congress has tried to impose controls on Internet speech to protect children, but so far its solutions have not passed muster with the courts.

Meanwhile, a number of initiatives have been launched that were designed to help educate adults about how to protect children when they go online. These projects and tools have included "Child Safety on the Information Highway," published by the National Center for Missing and Exploited Children and the Interactive Services Association in 1994, Project OPEN (the Online Public Education Network), organized by the ISA and the National Consumers' League in 1996, the Direct Marketing Association's "Get CyberSavvy" program in 1997, the American Library Association's "KidsConnect," as well as "America Links Up" and "Get Net Wise," both sponsored by a broad coalition of industry and non-profit groups. All of these initiatives have made useful contributions that educators and parents can continue to use to teach children "the rules of the road" when they go online.[4]

However, most of these projects dealt with technological solutions that were appropriate for a single computer, whether in the home or in the classroom. As school networks have grown to include dozens, if not hundreds or thousands of computers, there has been a need for additional information about how best to manage access across a larger network.

This briefing paper is designed to help school officials choose an approach that best meets their particular situation. Many schools have already taken steps to do so. Recent surveys indicate that approximately 98 percent of public schools that are connected to the Internet have adopted an Acceptable Use Policy. Seventy-four percent of schools with an AUP in place use blocking or filtering software, 64 percent make use of honor codes and 28 percent use an intranet to help control access.[5] As their networks continue to grow and evolve, schools

will continue to need authoritative information on their available options in order to make the best possible decision for their students.

What Is the Source of the Concern?

In the early 1990s, as the number of subscribers to proprietary online systems grew, transforming those communities from the moral equivalent of small towns to large cities or even states, children began to meet people in online chat rooms who would engage in inappropriate conversations or encourage them to divulge information about themselves. Then as proprietary systems such as America Online, Prodigy and CompuServe connected their users to the Internet, and more households accessed the Internet directly through Internet service providers, online users began moving easily to the wide open, unregulated spaces of the World Wide Web.

As the number of Internet users grew, the Internet changed as well. No longer was it a small, tightly knit community of academics, researchers and scientists, where all users generally supported an unwritten code of good behavior. With the advent of the World Wide Web, anyone could open up a store or publish a magazine. Because of the ease with which a Web site could be created—and displayed to a worldwide audience at virtually no cost—the number of individual sites on the Web has skyrocketed ever since.

Some experts argue that the Web is expanding so fast that it is virtually impossible to track every site that could be objectionable. The flip side of that argument is that it is better to minimize access to objectionable content as best we can, even if the occasional site slips through the cracks.

A related debate rages over what percentage of Web sites would truly be considered objectionable. Some advocates argue that sites that would be considered harmful to minors represent only a very small proportion of the Web. What is of greater concern, they say, is that perfectly benign and possibly very useful information could be blocked when software is used to screen inappropriate material.

For others, however, the actual extent to which adult-oriented materials are available on the Internet is irrelevant. Because it is possible for children to access such materials without the traditional-world protections of brown-paper wrappers or adult-bookstore doorways, they argue, the existence of any pornographic material is sufficient cause for concern. Those who support government-mandated content controls tend to argue that any amount of inappropriate content is too much, when children are concerned.

Pornography is not the only issue involved. Many adults are concerned about Web sites that are created by hate groups or devoted to topics such as bomb-making and weaponry, gambling or alcohol and smoking. Although pornography on the Internet has captured the greatest attention on the part of policy-makers, it is not the only area of potential concern for parents and educators.

How Big Is the Problem?

According to some estimates, the World Wide Web now includes 1.5 billion pages and new Web sites spring up at the rate of 4,400 per day.[6] Cyveillance, a company that monitors the Internet for business clients, estimated in July 2000 that the Web included 2.1 billion pages, with 7 million new pages created each day.[7] Many Web sites are abandoned, or rarely updated, but continue to persist on servers around the world, where anyone in the world can still access them.

In 1995, a study conducted by Marty Rimm, an engineering student at Carnegie-Mellon University, asserted that 83.5 percent of the pictures transmitted through UseNet newsgroups were sexually explicit. His findings were given additional credence when Time magazine featured the study in a cover story headlined "On a Screen Near You: Cyberporn!" Subsequently, the study was discredited and Time backed down from its story. But average Americans, not to mention members of Congress, were left with the perception that pornography could be easily found on the Internet, just a mouseclick away.[8]

Since then, a war of words and Web statistics has raged over the pervasiveness of material on the Web that would be considered inappropriate for children. Advocacy groups from the conservative end of the political spectrum contend that there are between 72,000 and 100,000 sexually explicit sites on the Internet and that 85 percent of the 3,900 new sites that are created each day sell commercial pornography.[9] On the other hand, another widely quoted 1999 study on the size of that part of the Web that has been indexed by search engines reported that 1.5 percent of a projected 800 million pages were pornographic.[10] Yet another study, by researchers at the University of Pennsylvania's Annenberg School for Communications, reviewed a random selection of Web pages turned up by a search engine and found that no more than 3.6 percent had "highly objectionable" material, only 2.4 percent had "provocative sexual content" and only 0.7 percent had "notable violent content."[11]

In July 2000, a representative of N2H2, a company that sells filtering software, told the Commission on Child Online Protection (the so-called COPA Commission) that it had categorized 4.7 million Web addresses, known as Uniform Resource Locators, or URLs for short, on its lists of sites that might be considered objectionable for one reason or another, including the display of pornography. That number translated into more than 15 million individual pages within sites. Further, the company said that it adds 20,000 addresses each week to its lists of sites that its customers could choose to filter.[12]

The World Wide Web, however, is not the only source of concern. Children can receive e-mail messages with pornographic file attachments and e-mail from UsetNet groups, which communicate through an older Internet protocol, can contain postings from users that would be considered inappropriate. Of special concern, too, are Internet chat rooms and so-called Instant Messaging, where children can communicate online in real-time with adult strangers who may not have their best interests at heart.

What Surveys Show

To what extent are children really encountering these kinds of materials or people?

In June 2000, a survey conducted for the National Center for Missing and Exploited Children found that one-fourth of children between the ages of 10 and 17 who regularly access the Internet said they had been exposed to unwanted online pornography in the past year. Most instances occurred, respondents said, when they were "surfing" and clicked on a hyperlink to another site, or searching the Web and mistyped the name of a Web site. About one-fourth of the instances were the result of e-mail that young people opened or Instant Messages that they received.[13]

The survey also found that 19 percent of the respondents had received an unwanted online request to engage in sexual activities or to provide intimate sexual information. Further, the report said, the young people or their parents rarely reported the incident, in part because they were not sure to whom they ought to make a report.

The staff at the Tacoma, WA, public library wanted to learn more about its patrons' experience with the filtering software it had installed. Using system logs, the staff tracked the demographics of library users, both adults and children, whose access to materials was blocked by the software the library used. It found that their median age was only 16 and that the age that generated the greatest number of intercepts was 13. Overall, the library found that about 6 percent of total sessions at public access terminals tried to access sites that were believed to provide graphic materials "depicting full nudity and sexual acts" for "sensational or pornographic purposes."[14]

A representative of the adult-oriented Internet industry told the COPA Commission in July 2000 that the records of Web sites reviewed by his group showed that 19 percent of visitors to the top adult-oriented Web sites were under the age of 15.[15]

How Concerned Are Parents?

If children apparently *are* accessing materials that could be considered inappropriate, how concerned are their parents?

America Online officials say that about two-thirds of their user households with children make use of the online service's parental controls features.[16] However, the National Center for Missing and Exploited Children found in its survey that only about one-third of the families used filtering or blocking software, including software offered by an Internet service provider. A survey conducted by the Annenberg Public Policy Center found a similar percentage of families that used filters, despite the fact that 76 percent of those parents said they were concerned that their children might view sexually explicit images on the Internet. (Interestingly, a greater percentage of parents (82 percent) were worried about what their children might encounter online when their families did not have Internet access.[17])

Similarly, a recent study conducted for FamilyPC magazine by Digital Research Inc. found that while 36 percent of parents felt there was too much violent content on the Internet, and 65 percent felt that "it's too easy to access sexually explicit information," 60 percent of them felt they "always know what my children do online." Thirty-four percent of parents in the most

recent study said their children had accidentally viewed inappropriate content, but 69 percent of the teens surveyed said they had seen such content. Sixty-four percent of the parents surveyed said they "personally checked" on their children and 55 percent said they "personally supervise activities." Twenty-five percent said they use blocking tools provided by their Internet service provider and 8 percent said they had purchased their own blocking software.[18]

Another recent survey of the general public found that while 71 percent believed the Internet could enhance their educational level and 86 percent said it would help their children learn more, there were still concerns about the kind of content that could be accessed. Seventy-six percent said they thought that "inappropriate content" could be a barrier to Internet adoption and 61 percent were worried about the potential impact of "dangerous ideas."[19]

The conclusion that some researchers have drawn from these surveys is that parents believe that the Internet can be an unsafe place, but are not particularly worried that their own children are getting into trouble. The children, it appears, are not always talking about what they are finding when they go online.

A Short History of Content Controls

As stories began to circulate in the mid-1990s about the negative experiences that children were beginning to have when they went online, there were two kinds of responses.

One was led by industry and children's advocacy groups, including educators. At the Fall Comdex meeting in 1994, the National Center for Missing and Exploited Children and the Interactive Services Association issued "Child Safety on the Information Highway," the first major effort to alert parents that they should monitor their children's online activities. Shortly after that, software companies began selling new products designed to address the concern. Others tried to limit access by developing rating systems to characterize Internet content, much the way theater owners limit children's access to movies that carry "R" ratings.

However, some members of Congress and conservative advocacy groups were reluctant to leave it up to the nascent Internet industry to regulate itself. They began to look for ways that the government could control children's access to inappropriate online content. This culminated in the passage of the Communications Decency Act as an amendment to the Telecommunications Act of 1996.

Ever since, both sides generally have stayed their particular courses, Internet businesses, education associations and civil libertarians tending to support voluntary solutions while more conservative advocates have supported federal and state laws to control Internet content as the best way of protecting children.

Development of Rating Systems

In 1995, SafeSurf, a self-described international parents' organization, implemented a rating system in which sites that agreed to meet certain standards would be included in a community of sites that were deemed to be appropriate for children.

A year later, after the first commercial software products began to appear, the Recreational Software Advisory Council stepped in to build on work it had previously done on rating computer game software. It adopted a system that enabled Web sites to rate themselves based on four categories of content: violence, nudity, sex and language. Sites could complete an online questionnaire that generated a metatag, a kind of invisible Internet nameplate that would characterize the nature of their content. An "i" was appended to the label when a Web site included interactive features that, because they involved real-time messages from site visitors, were beyond the ability of the Web site to control. Shortly after that, Microsoft and Netscape modified their browsers so that they could recognize RSACi labels.

Online policy experts and Internet companies realized, however, that labeling was an area that was fraught with political sensitivities. Groups might differ widely over what they would consider to be an acceptable Web site. Conservative religious organizations might, for instance, block access to Web sites that they felt promoted homosexual lifestyles while gay groups would not. Consequently, the Internet community felt there was a need for a rating system that could accommodate an infinite variety of standards and political perspectives.

Development of PICS

The PICS (Platform for Internet Content Selection) Consortium first convened in August 1995 to try to create this kind of "value-neutral" rating standard. The initiative, hosted by the World Wide Web Consortium at the Massachusetts Institute of Technology, included representatives of businesses, non-profit groups and academic institutions. Its goal was to develop a standard that could be used by groups of all political stripes to rate Internet content. In its vision, the National PTA could have a rating system, as could every group from the Moral Majority to the American Civil Liberties Union, if it chose to do so. Subsequently, the consortium adopted PICSRules, a protocol that was designed to let individuals communicate their content preferences to servers and search engines. Microsoft and Netscape incorporated the PICS standard into their 4.0 versions of the Internet Explorer and Navigator browsers, respectively.

Up to now, however, Web site labeling has not been adopted on a widespread basis. The Internet Content Rating Association, which has taken over promotion of the RSACi labels, is now focusing on encouraging adult-oriented sites, child-oriented sites and the 1,000 most frequently visited Web sites to adopt its labels in hopes of promoting them where they could theoretically make the biggest difference.[20] In December 2000, ICRA announced that it had expanded its rating categories beyond the four defined by its predecessor, and would enable Web sites to clarify the context in which their materials were presented. ICRA also announced it was incorporating the PICS standard into its labels.

In addition, the Entertainment Software Rating Board has rated about 280 game-oriented Web sites with a rating system based on age appropriateness.

However, at most, only about 150,000 sites have chosen to adopt one of the rating systems. It can be a time-consuming process for individual Web sites to review and rate their sites according to the rules of one system, much less others that could be developed. In addition,

some Web site owners, including traditional print publishers, have objected to ratings as an infringement of their free-speech rights.

As long as so comparatively few sites choose to rate themselves, an Internet user whose browser is set to access only sites that carry a certain rating will be able to access only a relatively small part of the Internet.

As Daniel J. Weitzner, the World Wide Web Consortium's Technology and Society Domain Leader, acknowledged during the COPA Commission hearings in the summer of 2000: "There is no clear incentive for sites to rate themselves. Most of the authors of the hundreds of millions of Web pages that now make up the public Web have not attached any content labels to their sites and have no clear reason to do so. Without some legal or market pressure forcing pages to be rated, publisher-controlled label systems are not likely to be effective." [21]

Development of Filtering Software

About the same time that Internet content ratings emerged, companies also began to market the first commercial filtering software products. Most of the early products were aimed at the home consumer market, and marketed to parents as a way of protecting their children. Products generally permitted access to either an approved list of Web sites or blocked access to a list of inappropriate sites.

From a handful of products in 1996, the market for filtering software grew to about three dozen products in 1997 and then to more than 120 when Get Net Wise prepared its guide to filtering products two years later. [22]

Software companies use a variety of approaches when they build their data bases of Web sites that should be blocked. Some have relied on what's known as artificial intelligence to scour the Web, looking for sites that contain "keywords" that suggest the content may be inappropriate for children. Critics have complained that this approach leads to "over-blocking" of sites that are not objectionable. Opponents of filtering have found instances in the past in which filtering products blocked references to chicken breasts and breast cancer research along with full frontal nudity, products that blocked references to persons holding "magna cum laude" honors or products that blocked, say, the home page of a town that just happened to be named "Middlesex." [23]

On the other side of the debate, those advocating "bullet-proof" protections for children have been more concerned about the potential for "under-blocking." They are concerned that with the rapid growth of the Internet, it is virtually impossible for a filtering company to review every new site. As the chairman of the COPA Commission mused at a commission hearing in July 2000, the process of keeping up with these sites must be akin "to trying to bail out an ocean of growth with a thimble."[24]

The major manufacturers of filtering software respond that they don't try to review every site—but that they don't have to. They say they use a combination of artificial intelligence "spiders" to cull through the Internet and identify pages that may be inappropriate and then

use teams of human reviewers to determine whether a site actually is. That way, they say, a site that is flagged because it provides recipes for chicken breasts would not end up on a list of sites that are blocked because they feature naked women.

Some stakeholders have also been concerned about the potential for blocking sites that are sensitive because of their political nature, such as sites dealing with homosexual lifestyles or political viewpoints that some groups may find offensive.

When filtering software was first introduced, most products restricted a very narrow range of categories, much like RSAC's initial four categories. In fact, when one filtering software company went into business in 1995, it had only two categories—"naughty" and "nice." [25] Since then, however, market considerations have driven the software industry to add a much wider range of categories that parents, schools and libraries can choose to block. In addition to material that is considered sexually oriented or violent, some filtering products screen for such things as hate groups, sites that promote gambling or illegal drug use, sites that teach visitors how to make bombs or acquire weapons and sites that contain advertising. In addition, some products that market to businesses who want to limit the personal Web surfing that employees do on company time include categories that can restrict access to online games, job searching and stock trading. With some products offering as many as 40 or even 60 different categories that can be blocked, adults who wish to set limits on children's access have many more options than they once did.

The Legal and Regulatory Backdrop

Despite the development of new software products, rating systems, and industry-supported online safety campaigns, Congress continued to regard the situation with alarm. In 1996, it passed the Communications Decency Act, which prohibited the posting of materials on the World Wide Web that would be considered "indecent" or "patently offensive." The legislation did not address the dissemination of child pornography or child stalking on the Internet, which, it was generally agreed, would be prohibited by existing laws. However, in 1997, in a decision known as *Reno v. ACLU* (or commonly as *Reno I*), the Supreme Court unanimously ruled that the measure was much too broad and amounted to an unconstitutional restriction on free speech.

Congress tried again the next year, passing the Child Online Protection Act, which made it a crime to communicate through the Web information that would be considered "harmful to minors" unless access was restricted through the use of a credit card. Violators could be subject to criminal penalties of up to $50,000 a day. In February 1999, a federal district judge blocked enforcement of the act, a decision that was supported by the U.S. Court of Appeals for the 3rd Circuit in a June 2000 decision known as *ACLU v. Reno III*. Once again, the judge ruled that the measure amounted to an impermissible restriction on free speech. Critics of the law noted that the legislation would have had no bearing on Web sites hosted on servers outside the United States, or on other kinds of Internet communications such as e-mail. In May 2001, as expected, the Supreme Court agreed to review the decision.

In overturning the Communications Decency Act in 1997, the Supreme Court made a distinction between that law and its position in a 1968 case, known as *Ginsberg v. New York,* which allowed states to restrict the dissemination of materials that could be deemed to be "harmful to minors."[26] In the past, these laws typically were applied to adult book and video stores, pornographic movie houses and convenience stores. But the Internet amounts to uncharted territory. Although many states have moved to impose restrictions of their own on Internet speech, so far these laws have not passed judicial muster. In August 2000, for instance, a U.S. district court judge in Virginia struck down a 1999 law in that state that attempted to restrict persons from selling, renting or lending sexually explicit pictures or texts to children online.

Opponents of laws such as the Communications Decency Act have generally promoted the voluntary use of filtering technologies as an alternative to government-mandated restrictions. Courts have upheld the rights of parents to protect their children from materials that they consider inappropriate. Many legal scholars believe that schools also have the right to choose to restrict their students' access to Internet content, at least during regular school hours, based on a Supreme Court decision in a 1982 case called *Board of Education v. Pico* that said books could be removed from a school library because of their "pervasive vulgarity," but not because of their "ideas."

In December 2000, Congress passed the Children's Internet Protection Act and Neighborhood Internet Protection Act (commonly referred to as CIPA or "the CHIP Act") as amendments to the fiscal 2001 appropriations bill for the U.S. Department of Education. This measure will require schools that accept federal E-rate discounts to purchase Internet access or internal connections or that use funding under Title III of the Elementary and Secondary Education Act to purchase Internet access or computers that access the Internet to adopt an "Internet safety policy" and a technology protection measure that blocks or filters content that is obscene, child pornography or "harmful to minors." The American Civil Liberties Union and the American Library Association, among others, have filed suit to block the parts of the law that apply to libraries.[27] CoSN has published information to guide school districts as they work to comply with the requirements of the law. However, for the purposes of this white paper, we will assume that a school district has unlimited choices and is not constrained by the requirements of the law. Because the law does emphasize some level of local decision-making, districts will be best served by working through these issues in a conscientious way at the local level.

Advocates on both sides of the debate seem to agree that government should do what it can to promote further technological developments to enhance filtering. Many believe that the government could help by providing the support necessary to evaluate the claims and capabilities of various filtering products in a vendor- and politically-neutral way. In its final report to Congress, issued Oct. 20, 2000, the COPA Commission recommended that the federal government take on this role.[28] The CHIP Act ordered the Commerce Department's National Telecommunications and Information Administration to undertake a study of the effectiveness of technological measures and Internet safety policies in schools, and to report back by the middle of 2002.

Content Management in the School Setting

Schools that decide they want to manage or monitor the Internet content that their students access can choose from a variety of approaches. The choice will depend in part on local community standards, the culture of the school or school district, the degree of control that teachers and administrators want to retain, the extent to which teachers and other school officials are willing to be involved on an ongoing basis, and, of course, cost. In evaluating its choices, a school district may want to consider whether different rules should be applied to children of different ages, and whether that kind of flexibility can be accommodated by the approach it wants to take.

This section will attempt to explain in layman's terms how these approaches work and pros and cons that various stakeholders may raise about them. Later, this paper will include a checklist of questions that school officials will want to review before making a decision on content management.

Acceptable Use Policies

Whether or not a school district ultimately decides to manage students' access to Internet content, it should still have an Acceptable Use Policy in place when they go online. Acceptable Use Policies are adopted by most Internet service providers, companies and other institutions that use computers to describe the behavior they expect of their computer users, the methods they will use to police that behavior, and the consequences if their rules are not followed.

The National Center for Educational Statistics reported in May 2001 that 98 percent of schools with Internet access had an Acceptable Use Policy in place.[29] In a 1997-98 survey of school librarians, 81 percent reported that their schools or media centers had such a policy in place.[30]

Acceptable Use Policies generally govern a wider variety of issues than just accessing non-instructional or inappropriate content. These may include such things as online copyright infringement, unacceptable uses of the school district's e-mail system and Web site, limitations on commercial use of the district's Internet resources, misuse of passwords, credit card and other forms of fraud and considerations related to student privacy and monitoring students' online activities.

Like many businesses, school districts may also decide to restrict their employees' use of Internet resources for both policy and financial reasons. The National Education Association believes that schools should adopt separate policies for staff members and students.[31] However, some schools may prefer to apply the same rules to all of their online users, no matter their age or status is.

The National School Boards Association, in a 1999 publication, advised school districts that an Acceptable Use Policy was "from a legal standpoint, the key to wisely harnessing the Internet's power." But, as with other decisions involving Internet usage, it noted: "No one

policy fits all. It is important for the school district to consider its size, how computers are used in education, what problems have occurred in the past, and how vigorously the finer details of the policy will be enforced."

The guidebook recommended that AUPs should not be too broad, because that can leave them open to legal challenge. But it said that the districts should also consider whether the AUP or general discipline policy should seek to punish students for off-campus behavior—such as creating a "hate site" directed at a teacher or classmate that could cause disturbances on campus. The publication provided a 17-point list of elements that should be included in an AUP.[32]

A number of sources that can be used to develop an Acceptable Use Policy are listed in the Resources section of this briefing paper. Typically, a student and his parent or guardian will be asked to sign the policy at the start of the school year. A good policy will spell out the consequences a student or staff member will face if the policy is violated. For instance, repeated violations of the policy might result in a student losing his Internet privileges for a specified period of time.

This kind of parental notification can take the form of an "Internet permission slip," in which a parent may be asked to give permission for his child to access the Internet, with an understanding of the things that may be beyond the ability of the school district to control. Schools might also decide to present parents with an AUP written at the level an adult could understand, as well as a copy of the policy their children will be asked to sign. Schools might even choose to craft different policies for different age groups, reflecting language and examples they would understand as well as the activities they are likely to be conducting on the Internet.[33]

The Children's Internet Protection Act requires schools that are subject to the law to adopt what it calls an "Internet safety policy" that addresses a number of issues, including online safety. A district must hold a public hearing and provide adequate public notice before adopting such a policy. [34] The Federal Communications Commission has said that if a school district's Acceptable Use Policy meets all of the requirements of CIPA, and was adopted after providing adequate public notice, it can suffice for purposes of the E-rate program.

An Opportunity for Learning

Some educators argue that instead of relying on filtering technology to block inappropriate content, schools should focus on teaching students how to evaluate Internet content and to form their own judgments on what is inappropriate. By relying on filtering software, they argue, schools may miss an opportunity to prepare students for what they are likely to encounter in an unfiltered environment, such as through their home computer, a friend's computer, a university network when they go off to college or a company's computer when they enter the workforce. Further, the rapidly evolving nature of the Internet virtually ensures that no filtering technology can be 100 percent perfect. Thus, even when a school uses a particular solution, children should be taught how to respond if they still manage to access something that it is inappropriate for them.

Further, the dangers that children can encounter online are not limited to off-color Web sites. Unsupervised chat rooms and so-called Instant Messaging functionality can enable adults to contact children, sometimes posing as children or offering enticements for further real-world contact. When schools begin accessing the Internet, with or without content controls, they should make sure that children are armed with the same kind of safety advice that parents and teachers would normally provide about the dangers of the traditional world: "don't talk with strangers and don't give out information about yourself." Online resources that can help teach these lessons are included at the end of this document.

Judith F. Krug, director of the American Library Association's Office for Intellectual Freedom, supported unfiltered access when she told the COPA Commission: "The children of today will be Net citizens for the rest of their lives. They need to be taught the skills to cope in the virtual world just as they are taught skills to cope in the physical world. Children should be educated in appropriate increments and appropriate settings on how to avoid inappropriate Internet content, to report illegal or unsafe behavior and to engage in safe interaction online. Children who are not taught these skills are not only in danger as children in a virtual world, they also will grow into young adults, college students and an American workforce who are not capable of avoiding online fraud, Internet addictions and online stalking."[35]

Whether or not a school district decides to use a technological approach to manage content, it would be well advised to promote "information literacy," that is, teaching children how to find good sources of information online and how to evaluate online information, as well as how to protect themselves when they go online.[36]

Monitoring

School districts may decide to adopt an approach in which they give students unlimited access to the Internet, but monitor the sites that individual students (or staff members) have accessed. That way an adult can respond if a student appears to be spending too much time accessing sites that are clearly beyond the scope of his or her schoolwork. Some school officials, however, may be troubled by this approach, fearing that it violates students' rights of privacy and smacks too much of "Big Brother."

Kevin Blakeman, president of U.S. operations for SurfControl, a developer of monitoring and filtering products, compared monitoring tools to a traffic officer, "who stands by the side of the highway and observes the situation, recording it and reporting it when appropriate."[37] The software can categorize the sites visited and files downloaded into pre-defined categories. It can document a range of activities, from excessive use to visits to sites that are believed to be inappropriate. This kind of approach is frequently used today in business settings.

If a school district employs monitoring, its Acceptable Use Policy should explain what it will be doing, and the procedures a student should follow if he or she encounters a site that would, by most standards, be considered inappropriate.

The Norfolk, VA, school district, for instance, uses a combination of filtering and monitoring tools to manage access on its network, which serves 37,000 students. The district's Acceptable Use Policy was created by a committee of parents, teachers and students, and then reviewed by the city attorney, who suggested some changes in the legal language. A student who has tried to access three blocked sites without reporting it to his teacher will have his Internet privileges revoked. Before regaining his privileges, he will have to take a refresher course on Internet etiquette and get his parents to sign a new copy of the Acceptable Use Policy. If students report that they tried to access a blocked site, the demerit is erased. When the system was first installed, Director of Information Technology Carolyn Roberson told the COPA Commission, the threshold was set at "10 hits an hour." But since then, she added, "students have come to know what's expected of them."[38]

Tools for monitoring usage can be purchased on a standalone basis or bundled as part of a filtering product. Certain kinds of network management products may also provide basic information on how students and staff are using the network.

Use of the monitoring approach naturally assumes that school district personnel will actually review system logs to determine if students and/or school personnel are abusing the system. Monitoring will make demands on staff time, so districts should make sure that they can manage this. It is probably worse to have the false security of a system that isn't used (or isn't usable) than to have no system in place. As noted before, districts that do decide to monitor should notify users that their usage will be reviewed, to stipulate what kinds of Web sites are considered off-limits and to make clear what the consequences of usage violations will be.

Schools that are subject to the CHIP Act because of the E-rate discounts they receive will be required to enforce an Internet safety policy that includes "monitoring the online activities of minors." At the same time, the legislation said the law should not be construed "to require the tracking of Internet use by any identifiable minor or adult user." Shortly before the CHIP Act passed, a New Hampshire Superior Court judge ordered a school district there to turn over its Internet logs after a parent, citing the state's "Right-to-Know" law, successfully sued to see them to determine whether children had been accessing inappropriate sites.

Filtering

In all of its forms, filtering involves providing access to a restricted number of Web sites. Access is either provided to a list of approved sites or access is blocked to a list of sites that are considered off limits. Generally speaking, the first approach will provide access to a much smaller number of sites than the second approach.

No matter which approach is used, someone ultimately has to decide which sites will be included on the list. Some teachers and school officials may want to retain complete control over that, but others will be willing to turn to third parties to manage the process for them.

Some filtering companies have been criticized for failing to explain what criteria they use when they decide to block a site. Before deciding whether to filter or whether to purchase a particular product, a school district should understand the criteria that a company uses to

evaluate sites. Most companies do not publish lists of the sites that they block, both for proprietary reasons and to deter potential hackers or children who might use such a list as a roadmap to find inappropriate sites on an unprotected computer. However, most reputable companies will provide some guidance on the criteria they use to evaluate sites.

School districts should try to determine whether a company's criteria would mirror the standards of their own communities. Many products permit an authorized person to provide access to an otherwise blocked site, or to let a school district set different access criteria for different groups of students. However, the more the product parallels the criteria that school officials themselves would apply, the less time teachers and other administrators will have to spend unblocking sites that they feel should not have been blocked or restricting access to sites that they feel should have been.

Filtering products also vary on how they alert a user that a site has been blocked. If a single site is requested, the user will usually be notified when the request is blocked. That makes it easier for authorized persons to override a blocking decision if there are reasons that it should be. However, the result may be different if a search engine is used. Blocked sites may appear on a results list, but cannot be accessed, or they may not be offered as a choice. Districts will want to consider whether they want students to know when sites have been blocked and if so, how that should be accomplished.

When filtering software was first developed in the mid-1990s, most of the available products were designed to be installed on a standalone home computer. While a school district could conceivably install filtering software on each individual computer, that approach doesn't make sense when a district needs to control access across a district-wide network. Nevertheless, school officials still have several options when it comes to devising a solution that can be implemented district-wide.

Proxy Servers

For many districts, a convenient solution is to install filtering software on the district's proxy server. A proxy server is the ideal place to do filtering for a network because it is the one point through which all network communications pass. In addition to evaluating and managing Internet content, proxy servers can also be used as a firewall, or protective shield, for a school district's network, providing protection from viruses as well as access by outsiders and hackers. Proxy servers also can produce data logs that can help monitor system usage and performance, whether or not they are used for content monitoring.

To manage content, proxy servers can either make use of a commercially available filtering product, or a school district can devise content controls of its own. In either case, the server will permit access only to a predefined list of acceptable sites or bar access to a list of sites that are deemed to be unacceptable. Filtering software installed on a server is far more difficult to disable than software installed on a standalone computer, either in the home or in school.

School districts can create their own lists of acceptable or unacceptable sites. But this is likely to be a time-consuming task that may end up producing less than satisfactory results. Most commercial solutions include a mechanism for lists to be updated regularly with the URLs of sites that were just created—or just discovered by Internet users. Some products also enable network administrators to set different access rules for different groups of users, and for authorized personnel to specify that certain users should be given access to an otherwise blocked site.

For instance, a particular software product might categorize sites that engage in "hate speech" and a school district might choose to block those sites. However, it might be appropriate for a high school teacher, in the course of a class on racism, anti-Semitism or the Holocaust, to let her class view some of those sites. Some products would allow her to unblock those sites so that designated members of her class could access them.

Servers can also be configured to recognize content labels such as the Platform for Internet Content Selection (PICS). However, because only a very limited number of Web sites have adopted these labels, this approach will provide access to a very limited number of sites. For instance, a district could decide to provide access to sites that were deemed acceptable under ICRA's rating system and other unlabeled sites that had been reviewed and approved by teachers. But the universe of sites that students could access for their research purposes would be only a fraction of the number that are available on the Internet.

Filtering on a proxy server can have an impact on network performance because of the need to match a URL against what may be a long list of blocked sites. The use of a caching server, which, in simple terms, permits a recently viewed site to be viewed again without having to send a request out beyond the district's network, can help speed access and reduce the bandwidth that would otherwise be needed. [39]

Application Service Providers

A relatively new approach in the education field is that of the Application Service Provider, a company that manages computer applications for school districts on the company's own servers. This approach is designed to save school districts from some of the responsibility and support costs of managing their own equipment.

Some companies that sell filtering software for school-based servers make the same products available on their own network of proxy servers through which schools can also access the Internet. In other cases, companies that position themselves as Application Service Providers may offer a variety of services, including Internet access and e-mail, on their own servers. School districts should evaluate the degree to which these approaches will give them the flexibility to adapt the content controls to their own needs.

Filtered Internet Access

Many Internet service providers that market to schools and families have adopted content controls of their own. Users may or may not be able to choose whether to use these controls, depending on how the service is deployed and marketed. In many cases, these ISPs are using

virtually the same product that schools and school districts can install on their own servers. In this case, the cost of the filtering software will probably be built into the ISP's monthly fees.

Some online services may offer several categories of access rights, tailored to children of different ages. If a child needs to access a blocked site, say, for a school research project, an authorized adult could change the child's access category to a less restricted one. However, that would give children access, at least temporarily, to a wider range of sites, rather than just the single site in question. While a school district may be able to decide whether or not to use the content controls provided by its ISP, depending on the service or product, it may not be able to modify those controls to meet the needs of an individual user or classroom.

School districts that access the Internet through a statewide or regional educational network may also find that that network has adopted a content-management solution of its own. Many networks are re-evaluating their policies in light of the passage of CIPA.

Portals and Search Engines

As the number of schools with Internet access has grown, so too has the number of search engines or portals aimed at the education market. These products are generally designed to frame or organize a student's Internet experience by greeting him with a classroom-oriented home page or a search engine that is especially designed for children and their interests. In some cases, a school district may be able to simply configure its systems to point to one of these Web sites as a starting point. In other cases, the arrangement may involve access to additional services and, possibly, fees.

Some products may offer school districts a free service in exchange for accepting the interface with messages or providing information about their users. Districts will want to evaluate these terms and conditions carefully to make sure they are compatible with the district's philosophy and, potentially, parental concerns. Sites that gather information about children are now subject to the Children's Online Privacy Protection Act and the role of schools in the administration of this law is still evolving.

In evaluating these portals and search engines, districts will also want to consider how restrictive they really are. For instance, does a search engine return a list of benign sites that nevertheless could contain links to inappropriate sites? Could a student access an inappropriate site through one of those links? If a student could, for instance, access an otherwise benign mass-market search engine through an education portal or a search engine aimed at children, would he then be able to access adult-oriented sites that have been indexed by the mass-market search engine? Administrators will want to evaluate whether a particular approach would let clever students access inappropriate sites through these sorts of "back-door" methods.

Green Spaces

New products are emerging that offer proprietary networks or intranets designed specifically for children. These solutions, sometimes referred to as "green spaces," are designed to try to create an enclosed, protected environment in which children can access a restricted amount of

content that is deemed appropriate for them. Generally speaking, however, they will provide access to a relatively small proportion of the millions of sites that are available on the Internet.

Not all of the "green space" type products are appropriate solutions for school-based servers. However, many content controls function in the same way. For instance, content controls provided by an online service provider can, in effect, create a restricted area for children within the provider's own network.[40]

An Observation

The lines between these different approaches are often blurry. Sometimes there will be true technological differences, but in other cases the distinction may be simply in how a particular product is marketed. Reduced to their most basic level, the options will differ in two important ways: 1) they will either allow children to access most of the Internet, except for sites that have been deemed inappropriate, or they will enable children to access only a relatively smaller number of sites that have been found to be appropriate; and 2) a school district may be able to modify a solution to fit its needs or it will have to accept choices that have already been made by others.

What the Future Holds

As with all aspects of technology, the tools and solutions for managing Internet content are continuing to evolve. But so too are the methods that unscrupulous Internet users and merchants can use to lure children to places and materials that could be considered inappropriate for minors.

So far, most of the focus of Internet filtering products—and government policy makers—has been on controlling access to obscene or pornographic Web sites. But that is only part of the content management problem. Children can receive e-mail with pornographic attachments. In addition, functions like chat and Instant Messaging, which children enjoy and which can promote interactivity, can also expose them to potentially dangerous adults, posing as children or sympathetic mentors, if the network is not restricted to children. Many products are beginning to address these problems and providing parents and educators with tools to limit children's access to them—or to provide greater assurances that the "friends" they meet in chat rooms are indeed children.

Unsolicited e-mail, or "spam" as it is commonly called, continues to be a problem for adults as well as children, not to mention system operators. An executive with a company that develops e-mail controls told the COPA Commission that it estimates that 91 percent of online consumers receive unsolicited e-mail, and the company's analyses suggest that about 11 percent of it is adult-oriented. Interestingly, consumers themselves estimate that as much as 25 percent of their unsolicited e-mail is adult-oriented.[41]

Another source of concern is about a practice known as "mouse-trapping," in which an Internet user requests a certain site, but is routed to another one, often featuring adult-oriented content. What makes this practice particularly onerous is that the user finds that the only way he can leave the site is to shut down his browser. The COPA Commission, for one, has

recommended that government regulators try to fight this practice through existing consumer-protection laws aimed at deceptive advertising.

Over the past few years, the focus of concern of policy makers and, indeed, Internet users themselves, has shifted to privacy considerations. During that time, the World Wide Consortium has been working on another project, known as the Platform for Privacy Preferences, or P3P for short, to design a standard that would enable an Internet surfer to signal to Web sites how his personal information should be used. There is a school of thought that this approach could be modified so that browsers used by children could be configured to signal that a user is a child and thus should be barred from adult-oriented Web sites, much the way an adult bookstore owner would bar minors in states where their access is prohibited by law. [42]

The process of controlling Internet content in the future will be complicated as Internet access migrates to new devices, such as personal digital assistants, pagers and cellular phones. If these kinds of devices begin to be widely used in school settings, product developers and educators will need to consider how to manage the Internet content that can be accessed through them.

In the meantime, government policy makers, advocates for children, Internet users and civil libertarians are likely to continue to battle over the best ways to control access—if it should be controlled at all. What all parties seem to agree is that government could help by providing the means to evaluate filtering technologies and products, so that parents, schools, libraries and businesses understand what the products can and cannot do. No fewer than three major government studies have just been completed, are in the works or have been proposed for the weeks and months ahead.[43] School districts should continue to monitor these initiatives, and developments in content management, to make the best possible choices for their students. This project will continue to work to keep school leaders informed about these issues and related developments.

A Checklist for Content Management Decisions

The Internet can be viewed either as a limitless resource that children should be free to explore or something that is fraught with hidden dangers and unscrupulous people from which children need to be protected. Depending on where a school district and local community fall along this continuum, they may make very different decisions on how to—and, in fact, whether to—manage the content that their students can access over the Internet.

Here is a checklist that school officials can use when they approach this kind of decision. The decision should involve all appropriate stakeholders, including teachers, parents, students, the technology and legal staffs, administrators, the School Board and the wider community. Each group will have different kinds of concerns that should be weighed in determining the right approach for a district to follow. These checklists assume that, despite federal legislation that would require most school districts to adopt technology control measures, school officials still retain some options.

Questions to Ask When Deciding Whether to Manage Content

✓How will students use the Internet?

The planning process for every school technology initiative should address this question. Is it anticipated that students will be using the Internet unsupervised, as a research tool? Or will teachers be managing their experiences more closely? How many computers are in classrooms, labs and media centers and how will that impact the ability of school staff to closely monitor how students are using the Internet? Answering these questions will help determine whether students' Internet access should be supervised and whether staff will be in a position to do it on their own.

✓Do you want students to be able to direct their own learning or is it more important for teachers to retain control of what goes on in the classroom?

To what extent does your school or school district foster a classroom culture in which students are independent learners? Or are you more comfortable with a more structured, more formal classroom model? How your school or school district answers this question will provide guidance on how comfortable you will be with giving students unrestricted access to the Internet.

✓Should different standards be applied, based on the age of the student?

Your district may decide that different approaches are appropriate, depending, say, on whether a student is in high school or elementary school. If so, you will want to make sure that your proposed solution will give you that flexibility. You may decide to adopt content controls only in certain schools, or you may decide to choose a product that will let you set different levels of restriction for different age groups or classes.

✓Should school employees be subject to the same rules as students, to their own set of rules or to no rules?

Are you concerned about how your employees will use the school district's online resources? If so, what kind of rules or limits do you want to impose? Should staff members be required to

follow the same rules that students do, or is it more appropriate to adopt a separate policy for adults? Should you distinguish between the kind of online activities they pursue during school hours and those that they pursue outside of school hours?

✓**Would you prefer to simply monitor how students and employees use the Internet, rather than blocking their access to sites?** Would this approach raise any privacy concerns? Will your staff have time to monitor these logs and respond to potential abuses?

✓**Are there other issues that you want to address at the same time?**
Some content management solutions address other concerns about the Internet or network operations. These include protecting a school network against hackers or viruses, protecting the privacy of students, and restricting children's exposure to advertising messages. If so, you may wish to evaluate whether a certain approach will provide a cost-effective solution to more than one problem.

✓**How will school officials respond if students are found to be accessing inappropriate material?**
This issue should be addressed in your Acceptable Use Policy. Students should know how they are expected to respond if they access a clearly inappropriate site, whether or not it was intentional.

✓**What strategies will your school district use to teach "information literacy?"**
No matter what approach a school district takes, it should ensure that its students understand the "rules of the road" when they go online and how to evaluate the content that they find there. These lessons can be imparted either as part of regular online classwork, or as special activities that must be completed before a student can go online.

Questions to Consider When Evaluating Content Management Products

✓**Who should make the decision on what kind of sites are blocked or accessed?**

If school personnel will make the decision on which sites students will be allowed to access, will they have enough time to devote to that task? How frequently will they be able to update their lists? Who will be responsible for updating the list of approved sites? Will that give students access to a wide enough variety of sites?

If a third party will make the decision on which sites will be blocked or accessed, do you understand the criteria it uses to evaluate Web sites? Does the organization or company have any particular bias? How easy will it be for school personnel to override those decisions if they disagree with them? How frequently does the organization or company update its lists of sites, and how easily is that update accomplished?

✓**What kinds of content are you concerned about?**

Are you primarily concerned about children's access to pornography and obscenity, or are you concerned about their access to materials on topics such as weapons, hate groups and alternative lifestyles?

✓**What has the experience been with the solution you propose to use?**
To what extent are children able to access inappropriate sites, either directly or through search engines and other links? If a product appears to be effective in blocking problem sites, does it go too far in also blocking sites that would be considered benign or needed by a class studying a sensitive topic? A team of staff members may want to test proposed solutions to see what kind of results they turn up. Research papers and testimony compiled by the COPA Commission provides information about the methods that have been used by other researchers to test the effectiveness of blocking software.

✓**How are users notified when they try to access a blocked site?**
Some products provide a clear notice when a site has been blocked. Some allow this message to be tailored to the network's needs. Some products block in a more invisible way. Is it important for your Internet users, both students and staff, to know if they have tried to access sites that were blocked? Or would you prefer that this information be withheld?

✓**Does the proposed solution address other forms of content besides just Web sites?**
Does it provide tools for controlling such things as e-mail, access to chat rooms, and Instant Messaging? Is it important for your solution to include that kind of functionality?

✓**How easy would it be for a child to hack into and disable a particular filtering solution?**
Generally, tools are more difficult to disable when installed on a server, whether it belongs to a school, an Internet service provider or a filtering company, than they are when installed on a desktop computer.

✓**Does the proposed solution incorporate advertising messages? Will third parties be able to collect information about how your students are accessing the Internet?**
Some products incorporate these features, sometimes in exchange for reduced fees, or no fees at all for the product or service. School officials should understand whether advertising or marketing messages are incorporated into a product and what information, if any, will be gathered about users, either individually or in aggregate. Sites that gather information about children are now subject to the Children's Online Privacy Protection Act and the role schools are expected to play in the administration of this law is still under discussion.

✓**If your students speak many different languages, does your proposed solution control access to sites written in languages other than English?**
Some children learn to subvert content controls by making their requests in a foreign language. Further, if a child's native language is something other than English, will he receive the same level of protection that a child typing in Web site names in English would?

✓**How will the proposed solution serve your district in the future?**

Will the solution still work as the number of Internet-accessible computers grows? How will that change the price? What future enhancements are on the drawing boards? If your district plans to let children access the Internet through other kinds of devices, how will you extend the controls to those products?

Related Resources

Children's Online Safety

"Safe & Smart: Research and Guidelines for Children's Use of the Internet," was published by the National School Boards Foundation in 2000. Available at http://www.nsbf.org/safe-smart/index.html.

"Get Net Wise. " This Web site, created in 1999 by the Internet Education Foundation, a coalition of education organizations, advocacy groups and Internet businesses, was designed to provide a safety resource for parents that was "one click away." It includes a useful guide to filtering software products as well as products that monitor children's online activities or that can set time limits on online sessions. Although most of the products are designed for single computers used at home, some of the products are identified as solutions for network servers. Available at http://www.getnetwise.org.

"Kids Connect" is a resource created by ICONnect, a technology initiative of the American Association of School Librarians, a division of the American Library Association. It is designed specifically to help school library media specialists, teachers and students. It is available at http://www.ala.org/ICONN/kidsconn.html.

The American Library Association's "Kids Connect @ the Library" provides resources primarily for parents, but also for children's librarians and school librarians. It can be accessed at http://www.ala.org/parentspage/.

"Parents Guide to the Internet," was created in November 1997 by the U.S. Department of Education's Office of Educational Research and Improvement and its Office of Educational Technology. It is available at http://www.ed.gov/pubs/parents/internet/.

"America Links Up: A Kids' Online Teach-in" was a 1998 public awareness and education campaign sponsored by a broad-based coalition of non-profits, education groups and businesses. Materials are available at http://www.americalinksup.org.

The Media Awareness Network is a project, sponsored by Canadian businesses and non-profit associations, designed to promote online safety and information literacy. It covers a wide variety of topics, including information literacy, Acceptable Use Policies, privacy issues, content management strategies and online marketing to children. Although the public policy information is from a Canadian perspective, much of the information could be useful for teachers and parents. The project's materials are available at http://www.webawareness.ca.

"Get Cybersavvy!," was an educational campaign for parents, children, educators and librarians that was created in 1997 by the Direct Marketing Association. The resources are available at http://www.cyberswavvy.org.

The National Center for Missing and Exploited Children has been involved with the online safety of children since 1994. Its Web site can be accessed at http://www.ncmec.org.

Safekids.com is a Web site created by Larry Magid, a syndicated columnist for the Los Angeles Times and a long-time advocate for child safety online. It can be accessed at http://www.safekids.com.

The Children's Partnership published "The Parents' Guide," a guide to help get children online and keep them safe, in 1998. It is available at http://www.childrenspartnership.org/pub/pbpg1.html.

Net Family News is a nonprofit news service devoted to serving the needs of teachers and parents working with children online. It helps distribute the news of a consortium of organizations working in this area. Its Web site and newsletter can be accessed at http://www.netfamilynews.org.

"Not in Front of the Children: 'Indecency, Censorship and the Innocence of Youth," by Marjorie Heins, discusses the history of efforts to try to protect children from content that was considered inappropriate for them. The book was published by Hill and Wang in May 2001.

Children's Internet Protection Act

The Consortium for School Networking will provide updates on the law and its requirements at www.cosn.org/resources.

The American Library Association has created a Web page to monitor developments associated with the law at www.ala.org/cipa. The ALA has announced it will file suit to block the implementation of the law.

Acceptable Use Policies

"Legal Issues & Education Technology: A School Leader's Guide," published by the National School Boards Association, 1999. This publication includes a listing of "Elements of an Effective Acceptable Use Policy (AUP) Governing Student Internet and Technology Access."

"Legal and Ethical Issues Related to the Use of the Internet in K-12 Schools," written by Dr. Nancy Willard, director of the Responsible Netizen project for the Center for Advanced Technologies in Education at the University of Oregon's College of Education. It is available at http://netizen.uoregon.edu/documents/policy.html. The home page of the project, which also deals with wider issues related to Internet ethics and behavior, is located at http://netizen.uoregon.edu/.

"Plans and Policies for Technology in Education: A Compendium (2nd Edition)," edited by Bagby, R., Bailey, G., Bodensteiner, D., and Lumley D. for the National School Boards Association, 2000. In particular, Chapter 7 provides useful information to school districts that need to create Acceptable Use Policies.

The National Education Association has prepared a "Technology Brief" on "Development of Student Acceptable Use Policies." It is available at http://www.nea.org/cet/BRIEFS/brief12.html.

The National Association of Secondary School Principals has published a legal memorandum entitled "The Internet, Students' Rights and Today's Principals," that discusses Acceptable Use Policies and other Internet issues. The December 1998 document is available on the organization's Web site, http://www.principals.org.

"Develop an 'Acceptable Use Policy' (AUP) for Schools and Public Libraries," compiled by The Internet Advocate. Available at http://www.monroe.lib.in.us/~lchampel/netadv3.html.

"Creating Board Policies for Student Use of the Internet," from "From Now On: The Educational Technology Journal," May 1995, edited by Jamieson McKenzie, Ed.D. Available at http://www.fno.org/fnomay95.html.

The Virginia Department of Education's Division of Technology has created a guide called "Acceptable Use Policies--A Handbook" that includes additional resources and templates for AUPs. It can be accessed at http://www.pen.k12.va.us/go/VDOE/Technology/AUP/home.shtml.

Some of the following references were created at least two years ago, and as a result, many of their links may no longer be working. Still, they may provide useful examples of Acceptable Use Policies that school districts and other entities have adopted. Acceptable Use Policies should be reevaluated every year to ensure that they remain current with the evolving legal and regulatory framework for the Internet.

"Technology Plans Resources Online: Acceptable Use Policies," compiled by NWREL's Northwest Educational Technology Consortium.
Available at http://www.netc.org/ tech_plans/aup.html.

"Critiquing Acceptable Use Policies," an essay by Dave Kinnaman, co-author of the book "Researching on the Internet." It is available at http://www.io.com/~kinnaman/aupessay.html.

Information Literacy

In addition to many of the sites listed above, the Web site of the National Forum on Information Literacy is a good starting point for learning more about this subject. It can be accessed at http://www.infolit.org.
The American Library Association has developed nine standards for measuring student information literacy. They are available at http://www.ala.org/aasl/ip_nine.html.

The ALA has compiled several resources to guide teachers, parents and students to age-appropriate Web sites. These include "700+ Amazing, Spectacular, Mysterious Wonderful Web Sites for Kids and the Adults Who Care About Them," a collection of links to sites that

have been recommended and organized by children's librarians. It is available at http://www.ala.org/parentspage/greatsites. Another is "Teen Hoopla: An Internet Guide for Teens," available at http://www.ala.org/teenhoopla/.

The Montgomery County (MD) Public Schools has created a Web site, "Electronic Literacy Pre K-12," to help teach children about information literacy. It includes templates to help evaluate Web sites, information about search strategies and search engines and lesson plans. It is available at http://www.mcps.k12.md.us/departments/isa/elit.

The University of Texas System Digital Library has created an online tutorial to test online information literacy skills. It can be accessed at http://tilt.lib.utsystem.edu/.

The Washington Library Media Association Online has compiled resources related to information literacy and lesson plans to help teach it at http://www.wlma.org/Literacy/infoskil.htm.

Filtering

The Commission on Online Child Protection (the COPA Commission) has compiled a variety of research papers that analyze both the extent of the online safety threat and the pros and cons of using various filters. These papers are available at http://www.copacommission.org/papers/.

Computer Professionals for Social Responsibility Filtering FAQ (Frequently Asked Questions). This document provides a good overview of filtering. It was last updated in October 1998. It is available at http://www.cpsr.org/filters/faq.html.

"Figuring Out Filters: A Quick Guide to Help Demystify Them," by Karen Schneider, School Library Journal, February 1998, available at http://www.schoollibraryjournal.com/articles/articles/19980201_5733.asp.

"Choosing a Filter That's Right for Your Schools," by Trevor Shaw, eSchool News, November 1999. Available through the magazine's archive at http://www.eschoolnews.org.

The National Academy of Sciences has launched a congressionally mandated study of filtering technologies. Provisions for the study were contained in the "Protection of Children from Sexual Predators Act of 1998." The study, which is being conducted by the National Research Council's Computer Science and Telecommunications Board and the Board on Children, Youth and Families, is scheduled to be completed by spring 2002. Information on the project is available at http://www.itasnrc.org.

"FilterGate, or Knowing What We're Walling In or Walling Out," by Art Wolinsky, describes the impact of so-called IP-Independent Virtual Hosting and Round Robin DNS on the operations of filtering companies. The article, which was published in the May/June 2001

issue of Multimedia Schools, is available at http://www.infotoday.com/MMSchools/may01/wolinsky.htm.

WiscNet, a statewide network serving educational institutions in Wisconsin, has developed a statement to explain its position on filtering to its members. It can be reviewed at http://www.wiscnet.net/filtering/policy.html.

Internet Content Rating Systems

More information on the history of the Platform for Internet Content Selection is available at http://www.w3.org/PICS.

More information on the Internet Content Rating Association and the RSACi (Recreational Software Advisory Council—interactive) rating system is available at http://www.icra.org.

More information on the SafeSurf labeling system is available at http://www.safesurf.com.

More information on the Entertainment Software Rating Board and its system for rating online games is available at http://www.esrb.org.

Content Management Technology

A good explanation of how proxy servers work is provided by "Web Proxy Servers," by Ari Luotonen, published in 1998 by Prentice Hall PTR. Luotonen is identified as the chief architect of the Netscape proxy server.

"Blocking Content on the Internet: A Technical Perspective," prepared by Philip McCrea, Bob Smart and Mark Andrews for Australia's National Office for the Information Economy. Although much of this document deals with networks in Australia, its discussion of blocking and filtering is useful for a wider audience. It is available at http://www.noie.gov.au/projects/consumer/content%5Fregulation/blocking1/blocking.htm.

[1] National Center for Education Statistics, "Access to the Internet" 1999. Summary available at http://nces.ed.gov/fastfacts/display.asp?id=46.
[2] "Children, Families and the Internet 2000," survey by Grunwald Associates. Summary available at http://www.grunwald.com/survey/newsrelease.html.
[3] Supreme Court in *Reno. v. ACLU,* June 26, 1997. The full text of the decision is available in many places on the World Wide Web, including http://www.ciec.org/SC_appeal/decision.shtml. The decision by a three-judge appeals court panel that preceded this decision includes an excellent description of the history of the Internet and content controls. It is available at http://www.ciec.org/victory.shtml.
[4] Links to many of these initiatives are available in the Resources section under "Children's Online Safety."
[5] National Center for Education Statistics, "Internet Access in U.S. Public Schools and Classrooms: 1994-2000," published in May 2001. Available through http://nces.ed.gov/. In its 1999 survey of technology directors, "Internet Usage in Public Schools," Quality Education Data found that 52.5 percent of districts that were connected to the Internet used filtering technology and projected that by the end of the 1999-2000 school year, 71.5 percent would use it. Its 2000 edition of the survey posed the question to teachers, who reported that 60.9 percent of their schools used filtering technology. (Twenty-three percent said they did not know.) A 1997-98 survey of school librarians found that 41 percent said their school or media center used filtering technology. The school librarians' survey was described in "How Do You Measure Up?" by Dr. Marilyn L. Miller and Dr. Marilyn L. Shontz, in School Library Journal, October 1999. Available at http://www.schoollibraryjournal.com/articles/articles/19991001_6686.asp
[6] Testimony of David Burt, founder, Filteringfacts.org, before the COPA Commission, July 20, 2000, citing David Lake, "The Web: Growing by 2 Million Pages a Day," in The Industry Standard, Feb. 28, 2000, available at http://www.thestandard.com/research/metrics/display/0,2799,12329,00.html. Burt now works for N2H2 Inc., a filtering software company.
[7] A press release on the July 2000 study is available at http://www.cyveillance.com/newsroom/pressr/000710.asp.
[8] The Time article on the Rimm study, and some of the critiques it spawned, can be reviewed on the Website of the Electronic Frontier Foundation at http://www.eff.org/pub/Censorship/Rimm_CMU_Time/. The hype surrounding publication of the article is also described in "Risk and the Internet: Perception and Reality," by Eric A. Zimmer and Christopher D. Hunter, which is available at http://www.copacommission.org/papers.
[9] Roberts, Crystal, "Internet Filtering and Blocking Technology: The Most Effective Methods of Protecting Children from Pornography," citing "Kids Online: Protecting Your Children in Cyberspace," (1998) by Donna Rice Hughes. The article by Roberts, a legal policy analyst at the Family Research Council, is available on the Web site of the Commission on Online Child Protection at http://www.copacommission.org/papers/.
[10] Lawrence, Steve, and Giles, C. Lee, "Accessibility and Distribution of Information on the Web," Nature400, July 8, 1999, pp. 107-09.
[11] Zimmer and Hunter.
[12] Burt.
[13] The survey was performed for the National Center for Missing and Exploited Children by the University of New Hampshire's Crimes Against Children Research Center. Details are available at http://www.ncmec.org.
[14] Testimony of David Biek, manager of the main branch, Tacoma (WA) Public Library, before the COPA Commission, July 21, 2000. The Tacoma library actually allows access to the texts of these sites, to parallel its policies regarding erotica.
[15] Testimony of Andrew Edmond, CEO, Flying Crocodile, Inc., before the COPA Commission, July 20, 2000.
[16] Testimony of Ginny Wydler, director of standards and policy, America Online, before the COPA Commission, July 20, 2000.
[17] Turow, Joseph, "The Internet and the Family: The View from Parents, The View from the Press," Annenberg Public Policy Center of the University of Pennsylvania Report Series No. 27, 1999.
[18] Testimony of Robin Raskin, editor of FamilyPC magazine, before the COPA Commission, Aug. 3, 2000.
[19] Findings are from a national survey conducted in 1999 and 2000 by the Digital Media Forum, a media policy consortium established by the Ford Foundation.

[20] Testimony of Sheridan Scott, member of the board of the Internet Content Rating Association, before the COPA Commission, July 20, 2000.
[21] Testimony of Daniel J. Weitzner, World Wide Web Consortium, before the COPA Commission, Aug. 3, 2000.
[22] Testimony of Lorrie Faith Cranor, senior technical staff member, AT&T Labs-Research, before the COPA Commission, July 20, 2000. Although Get Net Wise (www.getnetwise.org) is primarily designed to help parents choose an appropriate filtering product for their home, it can also be a useful resource for schools looking for a server-based approach.
[23] Some filtering companies have been criticized for blocking sites that share the same IP number as an inappropriate site. This practice is described in "FilterGate, or Knowing What We're Walling In or Walling Out," by Art Wolinsky, MultiMedia Schools, May/June 2001. It is available at http://www.infotoday.com/MMSchools/may01/wolinsky.htm.
[24] Comments of Donald Telage, chairman, COPA Commission, during the commission's hearing, July 20, 2000.
[25] Testimony of Kevin Fink, director of technology, N2H2 Inc., before the COPA Commission, July 20, 2000.
[26] This standard, often referred to as the "Ginsberg" standard, defines "harmful to minors" as any written, visual or audio matter of any kind that a) the average person, applying contemporary community standards, would find, taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; 2) the average person, applying contemporary community standards, would find depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, ultimate sexual acts, normal or perverted, actual or simulated, sado-masochistic sexual acts or abuse, or lewd exhibitions of the genitals, pubic area, buttocks, or post-pubertal female breast; 3) a reasonable person would find, taken as a whole, lacks serious literary artistic, political or scientific value for minors. Material must meet all three of the tests in order to be found harmful.
[27] The fate of the legislation will be followed on the Web sites of the Consortium for School Networking, www.cosn.org, as well as this project, www.safewiredschools.org.
[28] The COPA Commission's final report is available on its Web site, http://www.copacommission.org.
[29] NCES.
[30] Miller and Shontz.
[31] The National Education Association's guidelines for Acceptable Use Policies are available at http://www.nea.org/cet/BRIEFS/brief12.html.
[32] "Legal Issues & Education Technology: A School Leader's Guide," published 1999, National School Boards Association.
[33] A good example of an age-appropriate Acceptable Use Policy is one that the Plano, TX, Independent School District created online for elementary school children. It can be reviewed at http://k-12.pisd.edu/guide/elemen/index.htm. The district is planning to create additional guides for older age groups.
[34] More information on the requirements of the Children's Internet Protection Act are available at www.cosn.org or www.safewiredschools.org.
[35] Testimony of Judith F. Krug, American Library Association, before the COPA Commission, Aug. 3, 2000.
[36] The National Forum on Information Literacy is a good place to start for resources related to teaching information literary. Its Web site is http://www.infolit.org.
[37] Testimony of Kevin Blakeman, president of U.S. operations, SurfControl, before the COPA Commission, Aug. 3, 2000.
[38] Testimony of Carolyn Roberson, Norfolk (VA) Public Schools, before the COPA Commission, July 21, 2000.
[39] Luotonen, Ari, "Web Proxy Servers," Prentice Hall PTR, 1998.
[40] More examples of child-oriented portals and green spaces are provided in the "Resources" section of the National School Boards Foundation's "Safe & Smart" project, available at http://www.nsbf.org/safe-smart/resources.htm.
[41] Testimony of Sunil Paul, founder and chairman of Brightmail Inc., before the COPA Commission, July 21, 2000.
[42] This approach is described in "Zoning Speech on the Internet: A Legal and Technical Model," by Lawrence Lessig and Paul Resnick, Michigan Law Review, Vol. 98, November 1999, pp. 395-431, available at http://www.copacommission.org/papers/.
[43] In addition to the report of the COPA Commission, which was released on Oct. 20, 2000, the National Academy of Sciences was required by the "Protection of Children from Sexual Predators Act of 1998" to

complete a study of filtering technologies. The National Research Council is now undertaking that study, and expects to be finished by the spring of 2002. In addition, the Children's Internet Protection Act, which was passed in December 2000, requires the National Telecommunications and Information Administration to complete a study on the effectiveness of filtering and Internet safety policies by the summer of 2002.