Secure Computing Corporation's

SmartFilter ä

White Paper: Educational Market

Contents

SmartFilter ä : Education and the Internet: A Balanced Approach of Awareness, Policy, and Security

Introduction

Public and private schools at all levels are now realizing the benefits of the Internet as an educational tool. In order to prepare students for success in life and work in the 21st Century, academic leaders everywhere are working to implement more progressive programs for computer literacy. The Internet is a principal component for almost each one of these programs. However, the Internet was not conceived as an educational tool, and it is rapidly evolving as an unrestricted and uncontrolled source of content. Perhaps more than any other information resource, the Internet must be handled responsibly by both the community and the schools, so that students can utilize the best of the Internet without the risk of exposure to inappropriate material or potentially illegal or harmful situation.

This paper provides an overview of the Internet by evaluating its potential benefits and risks for education today. It also discusses practical guidelines for Internet use policies, and explores new software technologies that are being implemented in schools today to reduce or eliminate the downside risks of Internet use by students of all ages.

The Challenges for Schools "Getting Wired"

Academia's demand is growing for Internet connectivity. Within a typical school district system, regional and statewide educational organizations might be called upon to assist the school district superintendent, school leaders and the district's director of technology services to implement an effective district-wide computer network and Internet connection. The Internet offers a global "network" with no single governing entity, no checks on the kinds of information that is maintained, and no global restrictions it can place on the growing community of Internet users. Thus, "getting wired" poses a dilemma of control and liability for the school district.

To understand this phenomenon, it is important to become familiar with online systems and the technical services being provided by schools to their students:

- Online Services: These are commercial, self-regulated enterprises that facilitate a host of online activities from navigating cyberspace to exchanging files or electronic mail. These services provide "pass-through" access to the World Wide Web and other Internet protocols, and typically offer the capability to screen or provide some level of editorial/user controls of the material available on their systems.

- Bulletin Board System (BBS): Typically operated by individuals, businesses, or organizations with non-Internet (dial modem) connectivity. Many of these BBSs are now migrating to the Internet. Their material is usually oriented around a common interest or theme such as a hobby. Some BBSs

feature adult-oriented material, but these systems usually attempt to limit minors from gaining access to the material they contain.

- Usenet Newsgroups: An "electronic discussion group" focused on particular subjects or themes. Internet Relay Chat (IRC), a protocol popular in the educational environment, goes a step further to provide the ability to engage in "real-time" discussions online (from role playing to chess or bridge games). Increasingly, access to newsgroups and chat functions is taking place on the World Wide Web via HTTP. In the case of Usenet, this circumvents a school's ability to control newsgroup access completely or selectively.

- E-Mail: Enables students to communicate globally and to subscribe to or join "special interest" mailing lists to engage in group discussions on educational topics of interest. Some email servers will accept special commands via email to access other protocols (such as ftp download and UUENCODE graphics), and then return the data via email. And to some extent, LISTSERVs mimic Usenet discussion groups.

- Telnet: Allows users to log in or visit remote computers in search of specific information that may be stored there, or to run remote applications, or in some cases for BBS access.

- File Transfer Protocol (FTP): The standard mechanism by which students can download large files and even software programs off the Internet for their individual use.

Inappropriate Content on the Internet

Schools and other youth organizations are rightfully concerned about unwanted content such as sex, obscenity and pornography, hate speech, criminal skills, and gambling that is readily available to users of the Internet. Results of two recent studies (***Mehta-Plaza at New York University/Ontario,*** and ***Rimm at Carnegie Mellon***) suggest that commercial vendors of pornographic material are apt to post explicit pornographic material in public access newsgroups in order to attract new customers to their private, pay-per-use bulletin board services. Adult BBS owners reportedly post 71 percent of hardcore pornography, taking advantage of Usenet and other newsgroups as a vehicle for free advertising (***Rimm study***). These same studies also imply that the existence of unsavory content is growing.

Privacy and Censorship

At school as in the workplace, students should think in terms of "checking their privacy at the door" when accessing the Internet through the school's official Internet connection. They may have the privilege of using a classroom-wide, school-wide, or district-wide Internet, and therefore, they are held accountable to the policies and guidelines that apply to the specific group.

Last year, the Communications Decency Act was enacted as part of the Telecommunications Act of 1996. However, within months of its enactment, a panel of federal judges ruled that the indecency provision violated the Constitutional right to free speech. Like other Constitutional issues, free speech and freedom of expression on the Internet is an issue that is likely to be

embroiled in controversy, debate, and legal process for years to come. However, many school officials have found practical steps to move forward with the Internet connections while avoiding undue legal liabilities.

Guidelines for Schools

School administrators and technology coordinators are working to protect students and reassure parents that controls are in place to limit student/school access to appropriate Internet resources. One important step is the creation, implementation, and consistent enforcement of an Acceptable Use Policy, or AUP. An AUP is a written agreement clearly defining terms and conditions of Internet use, signed by school administrators, teachers, volunteers, and students and their parents. To be effective, the AUP should include specific acceptable uses and rules for "online etiquette" as well as access privileges and penalties for violations of policy. Because Internet use by students is a new frontier, it is imperative that schools explain (1). What material or sites it deems inappropriate, and (2). Online security issues and the illegality of hacking or attempting to gain unauthorized access to other computers. The AUP agreements should be signed by every person using the school's Internet connection, and should remain on file to serve as a legal and binding document. Violators of the school's AUP may receive a warning letter to the offending student and parents, with subsequent violations resulting in access restrictions or suspensions.

AUPs are still a relatively new idea, and it is incumbent upon every school system to ensure that its staff, its students and their parents are actively involved in the process of "going online." Everyone involved should come to understand what the Internet is, and how its teachers and their students will be accessing and using their Internet connection on campus or from home computers.

- School administrators should ensure that the school's Internet connection is implemented with adequate security features, provide Internet training for its teachers, and champion the AUP either as a unique document or as an amendment to the school's existing formal disciplinary policy.
- Teachers must take responsibility for their students' online activities in the classroom.
- Parents are responsible for their children's online activities while at home.
- Students are responsible for understanding the rules of the AUP and respecting the privilege of Internet use.

Guidelines for Parents: Awareness, Involvement, and Commitment to Policy

Parents who are not familiar with the Internet should make an effort to educate themselves. Most schools are more than happy to provide parents with orientation programs to demonstrate what students will be doing during their computer labs, including research and other activities on the Internet. More often than not, schools are hungry for parent volunteers to help in the computer lab, and their volunteer organizations usually provide free basic skills training to parents without prior computer experience in exchange for volunteer support.

Once a school chooses to set up an Internet connection and create an AUP, parents will be called upon to get involved, and should consider it a mandate to review the AUP carefully with their children so that both can provide informed consent and uphold the AUP. By the same token, if parents discover the school is providing Internet access without guidelines or provisions for keeping their system secure, they can and should take issue with school administrators to correct the situation as soon as possible.

Many schools have already laid the groundwork by creating AUPs, and making copies of their policies on the Internet. These can be used as a template and modified to suit each school's special needs. There are also mailing lists and Usenet groups through which you can post questions and share information and tips with other educators who have implemented AUPs at their schools.

Some useful resources for exploring AUP development include:

http://www.erehwon.com/k12aup/

http://www.rice.edu/armadillo/auppolicy.html

http://www.rice.edu/armadillo/aupenglish.html

http://www.netparents.org/

http://www.rice.edu/armadillo/About/bellingham.html

Following are some guidelines for parents and their children, based on information contained in a brochure written by Lawrence J. Magid for the National Center for Missing and Exploited Children and the Interactive Services Association:

- Children should never give out personal, identifying information (such as their location/address/contact information for the student, their parents, or their school).
- Remember that people online may not be who they seem.
- Remember that not everything one reads online is true.
- Parents should get to know the services their children use and encourage the children to let the parents know immediately if they come across any information or messages that make them feel at all uncomfortable.
- Children should be taught never to respond to message or bulletin board items that are suggestive, obscene, belligerent, or threatening or to provide their picture or anything else without first checking with parents.
- Parents can set reasonable rules and guidelines for computer use by children. This might include what time of day and how long a child is to be online and what areas are open for them to visit. Discuss these rules and post them by the home computer.
- If a parent becomes aware of the transmission, use, or viewing of child pornography while online, they should immediately report this to the National Center for Missing and Exploited Children by calling 1-800-843-5678. Also, they should notify their online service.
- Supervising adults should instruct children to obtain their express permission before arranging a face-to-face meeting with another computer user.

Policy Loopholes

Even the best policies can promote a false sense of security. Heavy-handed or loosely written, policies can be misleading and difficult to enforce. A well-managed Internet connection and a well-designed curriculum must balance the use of AUPs. Once students go online, other issues surface. Because chat rooms and newsgroups are typically poorly moderated, many schools avoid them. In addition, many schools set up their electronic mail as a semi-public system to help discourage inappropriate or harassing messages, and to proactively track down their perpetrators.

- *Client-based solutions* are sometimes chosen by small sites providing dial-up Internet access on a few stand-alone desktop or laptop PCs. Some school districts dependent on dial connectivity have employed these solutions, which apply machine-specific rules for basic access control, at an inexpensive cost. However, client-based solutions have proven untenable due to the difficulty in managing their use in the distributed, heterogeneous computing environments of many school systems today.

- *Server-based solutions* such as Secure Computing's **SmartFilter**, are tailored to "enterprise" use because they are implemented as a gateway on a single computer, independent of products on the desktop, whose use can be enforced. Larger school sites with LAN and dedicated connection environments and a mix of computer systems find server-based solutions more scalable, manageable and cost-effective over the long run. To support dial-up Internet access by a particular school, an Internet Service Provider can route the school access through a particular proxy server, and apply one set of access control rules for the entire school.

- *Ad Hoc solutions* are sometimes adopted by network administrators within an organization—using proxy, firewall, or gateway security software products—to block access to particular Internet Protocol addresses or URLs that must be identified and listed by the network administrator. This approach puts the burden of list development and monitoring on the network staff, which may not always be practical. Consequently, some network administrators are opting for dedicated security software solutions that provide a "subscription service" with a complete database of categorized URLs, and a host of powerful features such as timeframe-based controls and exemptions for selected individuals.

- *Stand-alone solutions* are among the first of a new breed of dedicated security solutions available. Products like **SmartFilter**, for NetCache simplify the otherwise complex task of URL filtering.

Stand-Alone Solutions—URL Filtering

URL filtering technology has emerged as the most suitable solution for protecting Internet connectivity within the academic institution, regardless of its size or the complexity of its access requirements. Therefore, a closer look at this approach and its application in a U.S. school system will be helpful.

URL filtering technology and products help customize Internet access for the classroom, the school, the district or the statewide school system, so that it becomes a safe, appropriate, and

productive resource to assist students in doing their schoolwork more effectively. From a database perspective, **SmartFilter**, provides a "logical view" of the Internet that can be tailored to the academic institution's particular needs. In other words, what is not relevant to a school's specific use of the Internet as an information resource simply does not appear to its users navigating the Net.

The **SmartFilter** Control List contains hundreds of thousands of categorized entries, sub-sites, and URLs, which include FTP, WWW and Usenet Newsgroup listings. The Control List, which is growing by thousands of sites each week, represents general content types encompassing an often wide variety of material that is deemed inappropriate for today's typical classroom. That is, in a standard classroom setting, this material is either non-education related, or inappropriate or both, and is therefore unproductive and potentially harmful for students.

Secure Computing offers this filtering technology on a subscription basis, delivering major benefits to schools. First, school network administrators can offload a virtually impossible task of continually maintaining and updating a massive database or Control List comprehensive enough to protect their students accessing the Internet. The **SmartFilter** Control List is updated continually with compiled updates available for download every week. Undesirable categories can be blocked based on installation parameters (schools select categories to block, and local additions and corrections to the subscription list are supported) as needed. Second, the school can reap substantial savings in human resource costs that would otherwise be required to provide Control List services onsite. Third, often-scarce Internet bandwidth can more easily be preserved for appropriate and productive use.

SmartFilter was designed for easy use by network administrators. The browser-based administrative applications simplify and speed the process of adding, removing, or reclassifying URLs and sites maintained in the Control List.

All URL access requests, whether successful or denied, are automatically logged by NetCache with convenient hyperlinks to visited/denied sites provided to the system administrator. The access log can be searched using several criteria: access attempt date/time, response received, and specific Internet Protocol address involved. Online activity can be monitored and evaluated across an entire school district's network server with NetCache logs. Daily server logs can be exported to PC-based spreadsheets and activity report tables and graphs can be easily incorporated into documents or e-mail to include a breakdown of categories of sites visited, types of files accessed, most active users, and busiest time periods for online access.

SmartFilter, on NetCache can be deployed in parallel to, in front of, or behind the computer network's firewall. The network is configured to require that all WWW, FTP, and Usenet News requests bound for the Internet pass through the NetCache proxy. All requests for URLs deemed inappropriate for the school system are refused.

Four factors impact successful maintenance and control of the database or Control List.

- Careful manpower management and oversight is required for sites that provide inappropriate content such as sex, illegal drugs, extreme/obscenity, criminal skills and activities, gambling, and hate speech. Schools, like many business organizations, generally opt to impose total blocking of these categories.

- Automated cooperative feedback from installations using a Control List helps establish and leverage a "network" effect, which makes it easier to maintain the quality of the database across a large installed base such as an entire school district.

- Human-computer interface tools that effectively support the efforts of Control List technicians are required to enhance productivity and reduce redundant efforts.

- Proprietary search and pattern-matching tools-or "robot-like" variations on those programs used to compile Internet search engine indices-help produce "candidate" sites for categorization following human review. Human review is vital in filtering out content typically resulting in too many "false positives."

Internet Educational Case Study: Omaha Public School System

The Omaha Public School System offers its 44,000 students in 80 different campus locations access to a wealth of educational resources available on the Internet. School district administrators chose Secure Computing's **SmartFilter**, an Internet monitoring and filtering software solution, to control student access to the Internet.

SmartFilter's Control List was adapted to the school district's specific educational guidelines in order to block access to inappropriate Web sites in 27 different categories including pornography, criminal activities, and hate speech. Administrators chose **SmartFilter** in part because of its server-based design, which simplified the task of defining and implementing a common set of Internet access control privileges that could be applied to the entire school district's network of client PCs from one central location.

Through this approach, the district realized significant savings in terms of administrative and budgetary resources that would otherwise have been required to handle each school individually. According to one school district administrator, "Our responsibility is to equip our students with the best, most modern tools for learning in preparation for their future. With the **SmartFilter** Control List, we can face parents with confidence, knowing that their kids are learning on the Internet exactly what they came to school for."

Conclusion

Undoubtedly, the world's academic institutions must embrace computer literacy and build it into their curriculum in order to prepare their students for the world that awaits them. And Internet access is an increasingly important part of the student's computer experience. It is incumbent upon academic administrators, teachers, and parents to introduce students to the Internet in a responsible fashion to ensure the best possible learning experience.

Access and use policies are vital, not just by virtue of their content, but in their universal acceptance. To support the application of access policies for responsible Internet use, technology solutions such as **SmartFilter** can be implemented as a method to customize the Internet for the educational environment and to provide a logical, relevant view of the Internet that is student-oriented.

Filtering technology provides a simplified, reliable, and cost-effective mechanism for schools to preserve the quality of the students' Internet experience.