

Responsible Internet Use

Steps to follow and advice to consider for protecting students from inappropriate material and helping them to be responsible Internet and Web users.

By Carol Truett, Allan Scherlen, John Tashner, and Karen Lowe

We are facing one of the great revolutions in the history of human communication. On a par with Gutenberg's invention of movable type, the Internet is expanding the concepts of freedom of speech and press virtually overnight. Issues in the United States concerning the First Amendment, individual privacy, and intellectual property must not only be reexamined but also kept foremost in our minds. U.S. citizens also have to realize that national laws and constitutional rights do not necessarily apply at the global level.

The Internet crosses national boundaries and is essentially ungoverned. Electronic citizens may have more of a voice in the cybernetic global village than they do in their national communities. For the first time in history an international dialogue goes on freely among individuals—seemingly unfiltered by governments, newspapers, or other organizations. Individuals can decide what they will read, see, or hear, and how they will let it affect their lives. Never in history has so much power shifted to the individual. It is no wonder government and religious leaders, not to mention local educators and school boards, have become concerned.

Internet Dangers Are Real

If you are using the Internet on a system without blocking software, it is easy to find sites that would bring shocked gasps to many parents and educators. By merely typing the word "sex"

in a Web search engine, you can find images of nude folks of both genders in a variety of situations that can be considered compromising at best. None of these pictures are ones you would want young students looking at during school hours.

Searching on the topic of AIDS, however, brings up potentially controversial sites, but ones that could also be very useful teaching aids for a health class. For example, one site details "How to Use a Condom," complete with diagrams and instructions to ensure safer sex. Keeping in mind that the Internet includes materials for all ages and levels of sophistication, this could prove to be lifesaving information for many individuals out there in cyberspace.

You can go further than that, however, and set up the computers in your school in such a way that no one can get access to anything potentially questionable. But if you block out terms such as "breast," your students have no access to information on breast cancer and other related topics. You can't give up one without the other. Here is some of the best advice and information

we have found available on the topic to help you make more informed decisions about your school's Internet-use guidelines.

Who Are We Trying to Protect?

We believe there are two categories of students to consider when we discuss censorship for children's sake. The first category constitutes those children who might accidentally stumble upon something vile and abhorrent through their innocent meandering through the Web. This group is actually the easiest to protect.

The second category of children is more problematic. These are the computer-savvy kids who actively seek objectionable material, send in the fake identifications, circumvent the blocking software, and are well-versed in the procedures for transforming binary files from e-mail documents into graphic images files. We need to protect these youngsters from themselves, at least while they are at school. We need to set responsible policies, procedures, and safeguards using such tools as Internet filtering software or rating systems, and possibly sharing some good advice with parents.

Tips for Responsible Proactive Use of the Internet

Many of the tips recently offered to parents by Gilliom (1995) can serve educators and librarians equally well. They include the following:

1. Be sure that curriculum objectives and goals for Internet use are

clearly delineated. Point students in the right direction. For example, when developing a class project, the librarian or teacher should check out appropriate sites well ahead of student use of the Internet. Sites can be bookmarked so that students won't waste valuable time searching sites that aren't useful, or wander way off base where they shouldn't be. A list of "acceptable" and "school-approved" sites can also be made available to all students and teachers.

2. *Get to know your students' online haunts and "friends."* Isn't this just a common-sense thing for all of us to do? Talk to students about what they search for on their own and observe them when they are using the Internet for school assignments.
3. *Never allow unsupervised surfing of the Internet.* A responsible adult should always be on hand when students are using the Internet in an educational setting. One recent article (Keeping Students in Line, Online, 1995) proposes that teachers assign students into groups of three to five to work on projects, because group members tend to monitor each other when online.
4. *Teach students Internet safety.* Warn them against giving out personal information such as telephone numbers or addresses, and encourage them to report interactive communications that made them uncomfortable.
5. *Teach youngsters that there are laws against harassment, and if they feel seriously threatened, they should report this to an adult immediately.* There are local and federal laws against harassment and threats online, and students as well as their teachers should be aware of them.

Internet Blocking Software

A recent article by Venditto (1996) offers an excellent discussion of software programs that help protect students from profanity on the Internet. The article profiles the two basic types of blocking software: filtering software and rating programs.

According to Venditto, filtering programs attempt to block material that the software's designer finds offensive, while at the same time allowing overall Internet access to continue. A database of banned sites is installed in the filtering program, and access to these banned sites is denied whether the Web address is typed in or a link is selected with a mouse. The database may also include lists of objectionable words that if used in a site would prevent access to the site.

Because of the constantly changing nature of the Internet, installing the regular updates is absolutely crucial to the method's success. Keeping your systems up to date can carry some expense—both in money for the updates and in time needed to install and troubleshoot them.

If you are going to use this method, be sure to check on how often the software is updated and what your charge for the new updates will be. Some are free. Other updates range from \$5–\$30 per month. The cost of the original blocking software is important too, although most are quite reasonable. Prices range from free to \$49.95 per workstation.

Rating Systems

Instead of allowing full access to the Internet with the exception of a few sites that are deemed objectionable, rating software permits access only to sites that have been given a positive rating. There are two main organizations that use this approach. The Recreational Software Advisory Council (RSAC) was formed in 1994 by a group of software publishing companies to help parents identify violent video games. RSACi has now developed an Internet rating scheme using a scale of 1 (least objectionable) to 4 (most objectionable) in four major areas—violence, sex, nudity, and language.

SafeSurf, the other software rating organization, was formed by a group of parents in 1995 to create a child-safe environment on the Internet. It uses a rating scale ranging from 0 to 10 points, with 0 indicating that the site contains nothing on the category being rated, and 10 indicating considerable objectionable content. The 10 categories or areas on which SafeSurf rates sites include the following:

- Profanity
- Heterosexual themes without illustrations
- Homosexual themes without illustrations
- Nudity and consensual sexual acts that may include illustrations
- Violent themes
- Both sexual and violent themes with profanity
- Accusations or attacks on racial or religious groups
- Themes advocating use of illegal drugs
- Other adult themes
- Gambling

While the RSACi ratings are quite specific within the areas rated, the SafeSurf system offers wider breadth of areas rated plus some finer discrimination in the system. The sidebar on page 55 gives more information on filters and rating systems.

Software Is Not a Cure-All

Although Internet blocking software and ratings system can be a big help in protecting students from inappropriate online material, a final caution is in order. These systems are still very new, and their success depends largely on the cooperation of the Web sites themselves. As Venditto (1996) says, "Both the RSAC and SafeSurf standards require that Web administrators rate their own pages. The only way parents and educators can get involved in the process is to prod Web administrators into rating their [own] sites" (p. 54).

Furthermore, when Venditto recently tested seven of the most popular blocking software programs in *Internet World*, he used the strictest level of control available for each program but could still only recommend three of them as excellent for blocking three main categories of objectionable material—drugs, sex, and violence. The three rated most highly were InterGo, Cyber Patrol, and Specs for Kids. (Contact information for each of these systems is available in the sidebar on page 55.) The bottom line on

these programs is that they are not foolproof and should not give educators or librarians a false sense of security that nothing objectionable will ever slip past them.

Acceptable-Use Policies

A third strategy for safer surfing of the Internet is an acceptable-use policy (AUP). An AUP is simply a written and sometimes signed contract between an Internet user and an Internet provider, whether the provider is a university, a school, or a commercial vendor such as CompuServe or America Online. The AUP states that the user will use the Internet only for certain delineated purposes. In schools, of course, these purposes are usually defined as educational and curricular.

AUPs perform certain valuable functions, including the following:

- Distancing school districts from liability.
- Informing parents and students that use of the Internet is a responsibility and a privilege.
- Easing the collective minds of teachers and media specialists.

AUPs do not, however, ensure that all student use of the Internet will be responsible. These contracts, like many others, may give everyone a false sense of security. Instead, AUPs may be far more valuable as a lesson in computer ethics and for teaching a sense of personal responsibility than as a guarantee that students will never abuse their Internet privileges.

It also appears to be the case that school boards and building administrators breathe easier with an AUP in place as a requirement for student Internet use. Although we have not yet heard of any school or school district being sued for some student's improper access to something on the Internet, it will certainly be interesting to see the outcome of such inevitable lawsuits and the role these AUPs play in protecting schools from liability.

What Should an AUP Contain?

At the very least, an AUP should inform students of the types of behavior that can get them or others into serious trouble (Rinaldi, 1994). These behaviors include:

- Placing unlawful information on the Internet.
- Using abusive or otherwise objectionable language in public or private messages.
- Sending messages that are likely to result in the loss of the recipients' work or systems.
- Sending "broadcast" or "chain-letter" messages to lists or individuals, or any other use that congests the networks or otherwise interferes with the work of others.

AUPs should be included as part of a school district's selection and collection development policy, and should be school-board sanctioned and approved. Nancy Willard (1996) provides an excellent online discussion in which she identifies several issues that a school board must address in creating an AUP. These include:

Resources for Creating Your Own AUP

The best way to create an AUP for your own school or district is to see what someone else has tried. The best source of sample AUPs is, not surprisingly, the Internet itself. Locate the following two sites on the Web and use the templates, examples, and guidelines that you find to make the job much easier. The print title listed is also a helpful resource.

School Librarian Links (<http://www.yab.com/~cyberian>).

This resource list for school librarians includes a large section on the subject of acceptable use and censorship. The area features a number of sample policies from actual school districts, including the California and Indiana state departments of education AUP requirements, as well as policies from individual schools such as Ben Franklin Middle School in Fairfax County, Virginia, and Oceanside High School in Oceanside, New York. This site also contains a link to the Classroom Connect AUP Frequently Asked Questions page as well as a comprehensive article entitled "What You Need to Know About AUPs," which features a template for creating a network AUP.

HISD's Armadillo Web Site (<http://www.rice.edu/armadillo/acceptable.html>).

This Web site, run by the Houston Independent School District (HISD) and the Center for Technology in Teaching and Learning (CTTL) at Rice University, includes an exhaustive list of articles on cyberporn and Internet freedom of speech, in addition to a sizable list of sample AUPs, including the one developed by HISD for its own use.

A Travel Agent in Cyber School: The Internet and the Library Media Program

by John F. LeBaron, Catherine Collier, and Linda D. Friel (1996, Libraries Unlimited, Englewood, CO). This recent book about the Internet is especially aimed at school librarians and contains an AUP from the Nueva School in Hillsborough, California, which is particularly noteworthy for its use of nontechnical and straightforward language.

- The educational purpose of Internet access.
- District versus parental responsibilities.
- Technical services provided through the district system, such as whether or not blocking software will be acquired.
- Access issues, such as Web access, group accounts versus individual accounts, and dial-up access from home.

Willard also provides an excellent explanation of students' rights to information and First Amendment protections. For other resources in developing AUPs, see "Resources for Creating Your Own AUP" on page 54.

Williamson (1996) suggests that most K-12 AUPs should include the following five components:

1. A brief explanation of what the Internet is and why it is being made available in school.
2. A warning that adult materials are on the Internet and can be purposely or accidentally accessed.
3. A reminder that Internet access is a privilege, with a description of what is and is not acceptable use.
4. The specific consequences of violating the AUP, which may include anything from revoking the student's Internet privileges to school disciplinary or legal action.
5. A disclaimer regarding the school district's responsibility.

Conclusion

When in doubt, remember that your library or computer lab offers Internet access for educational—not public—use. Unlike a public library, school libraries exist to support specific curricula; they are not intended to provide information on every topic imaginable. After all, you wouldn't buy just any old books—paperback smut and all—to place in the school library media center or a classroom. ■

Carol Truett (truettca@appstate.edu) and John Tashner (tashnerjh@appstate.edu), Reich College of Education, Department of Leadership and Educational Studies, Appalachian State University, Boone, NC 28608; Allan Scherlen, Belk Library, Appalachian State University, Boone, NC 28608; and Karen Lowe (lowekr@appstate.edu), Northwest Regional Educational Service Alliance, 201 Curtis Bridge Road, Wilkesboro, NC 28697.

References

- Gilliom, G. (1995). When your kids are online. *CompuServe Magazine*, 14(12), 12-21.
- How to write an acceptable use policy. (1995). *Classroom Connect*, 2(2), 16-17.
- Keeping students in line, online. (1995). *Classroom Connect*, 1(3), 12-13.
- Rinaldi, A.H. (1994). Conduct becoming an internaut. *Classroom Connect*, 1(2), 12-13.

Venditto, G. (1996). Safe computing: Seven programs that filter Internet access. *Internet World*, 7(9), 49-58.

Willard, N. (1996). *A legal and educational analysis of K-12 Internet acceptable use policies* [Online]. Available: www.cyberethics.com.

Williamson, C. (1996). Another look at acceptable use policies. *Technology Connection*, 3(2), 23-25.

Internet Filtering Software

Cyber Patrol. WWW: <http://www.microsys.com/cyber/default.htm>; e-mail: cyberinf@microsys.com. Available for Windows/Macintosh. Cost: \$29.95 per copy, which includes a three-month subscription to the Cyber NOT blocking list. Additional one-year subscriptions cost \$29.95. Educational discounts are available for orders of 10 copies or more. Prodigy and CompuServe customers can use Cyber Patrol for no additional charge.

InterGo. WWW: <http://www.intergo.com/tour/tour.htm>. InterGo is a complete Internet software solution, which includes a Web browser and an e-mail and newsgroup program. InterGo has a feature called KinderGuard, which blocks locations containing objectionable materials. The cost for the entire software package is \$49.95 per copy.

Specs for Kids. WWW: <http://www.newview.com>. Available for Windows 3.1, 3.11, 95, and Sega Saturn.

Internet Rating Systems

RSACi. WWW: <http://www.rsac.org>. Microsoft's Internet Explorer 3.0 browser software uses the RSACi system in its Content Advisor feature. CyberPatrol also uses RSACi.

SafeSurf. 76032 Sherman Way #58, Van Nuys, CA 91406; 818/902-9390; 800/720-3638; WWW: www.safesurf.com. SafeSurf actually rates sites and filters inappropriate sites. The SafeSurf Internet Filtering Solution is available through your Internet provider for a fee. It supports Unix and DOS-based systems. The filtering software is engaged the moment a "child's" password is used. The filtering software only accepts information from rated Internet sites.