Safety on the Net

Out on a Lim With Educational Technology

BY JANINE LIM

In the previous column, we discussed ways to guide and organize student research on the Internet. However, another issue relating to Internet use in schools is that of *safety*. How do we keep our children safe and yet teach them the information literacy skills needed to survive in today's fast-changing world?

There are, of course, many beneficial resources on the Internet such as reference information, access to stock trading, travel reservations, banking and shopping, easy communication with family and friends, and the ability to learn about virtually any topic.[1] However, as in any other environment, children can be targets of crime and exploitation. Young people are trusting and curious. They are quick to explore the new world of the Internet and all it has to offer. And so they need "parental supervision and common sense advice on how to be sure that their experiences in 'cyberspace' are happy, healthy, and productive."[2] A caution penned a century ago applies even now: "Eternal vigilance must be exercised, that the children may be led in the paths of righteousness. Satan begins his work upon them from earliest childhood and creates desires for that which God has forbidden. The safety of children depends largely upon the vigilance, watchfulness, and care of the parents over them." So let us look at some ways that teachers and parents can watch over God's children.

Acceptable Use Policies

The first step in our defense of children is to develop a school Acceptable Use Policy, otherwise known as an AUP. An AUP includes a description of unacceptable uses within the following areas suggested by Nancy Willard, an Information Technology Consultant:

- Personal Safety
- Illegal Activities
- System Security
- Inappropriate Language
- Respect for Privacy
- Respecting Resource Limits
- Plagiarism and Copyright Infringement
- Inappropriate Access to Material[4]

The AUP can be integrated into the school's registration process. Students and parents can be asked to read and sign the form at the beginning of the school year and keep it on file. Students who have not signed an AUP should not get computer access.

Schools should post the rules indicated in the AUP next to the computers in their classrooms, labs, and libraries. Or better yet, they can put the information on their mouse pads, so students have no excuse for not knowing the rules.[5] The National Center for Missing and Exploited Children suggests the following rules:

- I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.
- I will tell my parents right away if I come across any information that makes me feel uncomfortable.
- I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.

Picture Removed

- I will never send a person my picture or anything else without first checking with my parents.
- I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do, I will tell my parents right away so that they can contact the online service.
- I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.[6]

Along with posting such rules, schools should develop rules and conse-

Continued on page 46

Safety on the Net

Continued from page 31

quences for those who disobey the guidelines. School personnel should monitor computer use to help students follow the rules.

Educate Parents and Students

The next line of defense is to educate parents and students on how to safely use the Internet. The following activities are examples of ways to teach computer ethics. They were suggested by Doug Johnson, director of media and technology in the Mankato Public Schools in Minnesota:

- Articulate values.
- Reinforce ethical behaviors and react to non-ethical behaviors.
- Model ethical behaviors.
- Create technology environments that help students avoid temptations.
- Encourage discussion of ethical issues.
- Stress the consideration of principles rather than relying on a detailed set of rules.[7]

Educators should keep informed about Internet safety by reading articles about the Internet and its dangers and benefits.[8] Here are some ways to sensitize students to the perils of Internet use: Use real-life situations to start discussions, tying the examples to similar situations in the physical world where students already know how to make decisions about right and wrong.[9] Have students take an online quiz such as the one provided by CyberAngels to determine whether they understand the issues.[10] Or use programs such as the CyberSmart School Program[11] or Classroom Connects Internet Driver's License.[12]

Filtering Software

Finally, schools should consider installing software or a firewall to filter what students can access on the Internet. There are many options for both small and large schools and colleges. Filters can block sites that feature pornography, violence, hate speech, gambling, and drugs. However, filters also have their limitations. "The lists of banned sites which are 'blocked' become dated almost as quickly as they are distributed. Since listing individual pages is onerous, the programs tend to block entire servers resulting in inaccessibility to huge blocks of suitable information. One program blocks a huge California web server just because of the classified ads it carries."[13]

Even with these limitations, blocker software can be one of your best defenses to protect children from inappropriate material. Several software packages are available, as well as reviews to help you make your choice.[14] But remember that software will never be as smart as a human being. Nothing can replace monitoring of students and providing guidance and direction for their time on the Net.[15]

There are no perfect answers, but if we educate ourselves and our children, we can help protect them from the evil in the world. We should also remember that "[t]he only safety for the youth in this age of pollution is to make God their trust. Without divine help, they will be unable to control human passions and appetites. In Christ is the very help needed, but how few will come to Him for that help. Said Jesus when upon the earth, 'Ye will not come to me, that ye might have life.' In Christ all can conquer."[16]

***Janine Lim** is the Instructional Technology Consultant at Berrien County Intermediate School District in Berrien Springs, Michigan. She works with Adventist schools as well as other private and public schools.*

NOTES AND REFERENCES

1. Lawrence J. Magid, "Child Safety on the Information Superhighway" (1994). http://www.internetalliance.org/project-open/child.html. Accessed November 30, 1999.
2. Ibid.
3. Ellen G. White, *Child Guidance* (Washington, D.C.: Review and Herald Publ. Assn., 1954), p. 474.
4. Nancy Willard, K-12 Acceptable Use Policies. http://www.erehwon.com/k12aup/board_policy.html. Accessed November 30, 1999. To see an example of an Adventist school's AUP, visit http://www.nilessda.org/school/aup.html.
5. Visit http://adgraph.home.texas.net/Mousepads/mainpage.htm to find information on a company that prints AUPs on mouse pads.
6. Magid.
7. Doug Johnson, *Ethical Issues Surrounding Technology Use in Elementary Schools* (November 11, 1998). http://www.isd77.k12.mn.us/ethics.htm. More teaching suggestions can be found at: http://www.computerlearning.org/Articles/Ethics98.htm.
8. To get started on your reading, see "Internet Safety: Protective Gear for School," *Curriculum Administrator* 35:11 (November 1999), pp. 46-53; and visit http://cyberangels.com/childsafe.html and read about Child Safety. Then visit The Internet Advocate to learn about the issues: http://www.monroe.lib.in.us/~lchampel/netadv.html. Also visit ZDNet's family safety column: http://familypc.zdnet.com/safety/index.html.
9. Find examples at http://www.isd77.k12.mn.us/ethics.htm and http://www.computerlearning.org/Articles/Ethics98.htm.
10. See http://cyberangels.com/quiz/quiz.html.
11. See http://www.cybersmart.org/modules.htm. The creator of this resource, Jim Teicher, also published an excellent article in the February 1999 issue of *Educational Leadership*, "An Action Plan for Smart Internet Use" (56:5), pages 70 to 74.
12. Visit www.classroom.com and choose Online Store, then Internet Basics for Students.
13. Doug Johnson, *Internet Filters: Censorship by Any Other Name?* (January 15, 1998) at http://www.isd77.k12.mn.us/resources/dougwri/filter.htm. Accessed November 30, 1999.
14. See ZDNet's FamilyPC article: http://familypc.zdnet.com/safety/filtering/feature/21de/ which reviews Cyber Patrol 4.0, Cyber Sentinel, Cybersitter, SOS Kidproof, SurfWatch, Web Chaperone, and Net Nanny 4. Also see Cyber Angels chart comparing Cyber Patrol, Cybersitter, and Net Nanny at http://cyberangels.com/safetyandprivacy/chart.html. My workplace uses X-Stop to provide filtering for more than 20 school districts and 30 private schools in three counties. See http://www.xstop.com/ for more information on server-based filtering.
15. If you missed my previous column on Internet research, you can read it at http://www2.andrews.edu/~freedj/jae.htm.
16. White, *Child Guidance*, p. 467.