Online Safety: Striking A Balance

On the one hand...

We've all seen it in the news: online predators trolling for young victims; innocent Web surfers having their identities stolen; personal information culled and distributed; and pornographic images popping up unexpectedly or found readily by minors. You'd think the Web was a virtual Sodom and Gomorrah.

As an educator in today's digital age, you need to understand the liabilities that you and your school face whenever: electronic mail is sent from school computers, school members receive unsolicited email (think "hostile work environment"), and sensitive personal information is inadvertently published on school Web sites. While any of these could bring lawsuits to your school, student safety is, of course, of paramount concern. Consider these statistics published by the National Center for Missing and Exploited Children:

- One in four regular Internet users younger than 17 was exposed to unwanted sexually oriented pictures on-line during the past year.
- One in five youths receive an on-line sexual solicitation or approach during the past year.
- One in 17 was threatened or harassed on-line during the past year.
- One in 33 received an aggressive sexual solicitation on-line involving offline contact or a request for offline contact during the past year.

On the other hand...

According to a study by the University of California, Irvine and the University of Minnesota ("Internet Use by Teachers," Henry Jay Becker, 1999), there is a direct correlation between the use of technology and achievement in the classroom. Email, in particular, proved to be a valuable tool in the learning environment. In fact, "Across almost all subject-areas, electronic mail was used more by high-achieving classes than by low-achieving classes." In the report, fully 87% of teachers reported believing that having a computer with email was "valuable" or "essential." So how do you strike a balance between safety and access? There *are* ways to limit your liabilities while still providing critical online tools.

Limiting your liability

Your school or district may be liable for use -- or abuse -- of whatever online communication system has been put in place -- whether it's been set up in-house, outsourced, or consists of "free" online services. Even if your district doesn't receive federal funding for technology, it greatly behooves any superintendent or tech director to at least:

Adopt an Acceptable Use Policy (AUP) that addresses Internet safety in a meaningful and workable way. For questions about liability, consult your school counsel. For more information, visit the Northwest Educational Technology Consortium which features helpful guidelines and sample AUPs.

Know the Full Capabilities of Your Filtering or Blocking Software—and recognize that it probably doesn't work quite as well as you would like it to. Current consensus is that these mechanisms are far from perfect and are apt to block valuable research sites capriciously. Try to find software or services that will allow the most flexibility and customization. Regardless, your district must implement filtering or blocking as per CIPA, and certify *by October 28, 2001* that it has taken steps toward CIPA compliance in order to receive federal funding like E-rate or ESEA. For some good information about filtering and blocking software and services, visit this *Electronic School* article.

Involve the Community; for those schools depending on E-rate or ESEA funding for technology, they must publicize and hold at least one public meeting to discuss Internet safety (per CIPA requirements) in order to certify compliance and protect their funding. In general, it's a good idea for the community to be involved with issues like Internet safety because students use computers before, during, and after school. Combining the resources of both the school and the parents makes sense from an Internet safety standpoint.

The Internet has far too much to offer our students for us to indiscriminately block their access to it. And online communication -- email in particular -- is far too useful a collaboration tool in this modern age for us to deny its use for our students. The trick is to find solutions that help balance safety and substance.

Below, you'll find some useful, practical information on email safety and what to do if you encounter criminal activities via the Internet in your school. By the way, thanks to many of you for your encouraging feedback and excellent suggestions.

Torrance Robinson
President & Co-Founder
eChalk

Email Dos and Don'ts

DO: Install an anti-virus program on desktop computers to prevent viruses from spreading via floppy disks.

DO: Make sure your communication platform automatically scans incoming email for viruses.

DO: Consider a communication system whereby school- or district-wide email can be "closed down" so that students can only send and receive email from within the school community.

DO: Look at the file extension of the attachment: if it ends in: .pif, .lnk, .com, .bat, .doc, or .exe, then it may be a virus.

DON'T: Open a file attachment if you have any doubt about whether it is a virus. Ask the sender to verify the email's legitimacy.

DON'T: Automatically think it's okay to set up all your students with a free, Web-based email account. Not only are many of these companies sharing and/or selling user information, but they are also letting a good deal of porn-related spam to get through unsolicited.

What to Do If Someone is Soliciting Students Online
You should immediately contact your local or state law enforcement agency, the FBI, and/or the National Center for Missing and Exploited Children. Also, turn the computer off in order to preserve any evidence for future law enforcement use. You should not attempt to copy any images or text found, unless advised to do so by the law enforcement agency.

What to Do If You Suspect Identity Theft
Again, you should contact your local law enforcement agency, as well as your credit card companies, credit reporting bureaus, banks and creditors. To submit a report to the FTC, you

can use their Identity Theft Complaint Form. You can also forward unsolicited commercial email (or spam) directly to the Commission using this email address uce@ftc.gov.

What to Do If You Suspect Fraud or Misuse on the Internet
The Federal Trade Commission enforces a variety of consumer protection laws and is maintaining a database of telemarketing, identity theft, and other fraud-relating complaints for use by civil and criminal law enforcement agencies worldwide. While the FTC does not resolve individual consumer problems, your complaint helps them investigate fraud and can lead to law enforcement action. Visit their Consumer Sentinel page for more information.

Useful Links

The FBI's "Parent's Guide to Internet Safety"
http://www.fbi.gov/publications/pguide/pguide.htm

National Center for Missing and Exploited Children
http://www.missingkids.com/

Test your younger students' Internet safety savvy
http://www.missingkids.com/quiz/internetquiz.html

ABOUT THIS PUBLICATION:
eChalk Reports is distributed electronically by eChalk, a leading Web-based communication service provider for K-12 schools. Topics addressed are presented with the purpose of bringing greater clarity, focus, and balance to some of the current and growing trends in education technology. If you have any questions about this newsletter or would like to suggest a topic to be covered, please send an email to feedback@echalk.com. To read past issues of *eChalk Reports*, click here.

ABOUT eCHALK:
eChalk is the leading provider of integrated, Web-based communication platforms for K-12 schools and districts. eChalk offers each school its own secure, affordable, easy-to-use and entirely advertising-free network, which includes email, school directory, online classrooms, file storage, calendaring, Web publishing tools, and ongoing support. As an Application Service Provider (ASP), eChalk leverages schools' existing technology infrastructure and requires no new hardware, software or technical staff time. The company's mission is to enhance the educational process by providing highly effective communication and collaboration tools to students, teachers, parents, and administrators.

Copyright (c) 2001 eChalk, LLC. All rights reserved. eChalk and the eChalk logo are registered trademarks of eChalk, LLC. All other trademarks mentioned herein are the property of their respective owners.