The following document is from:

Safe and Responsible Use of the Internet: A Guide for Educators

Nancy E. Willard, M.S., J.D.

Responsible Netizen Institute
474 W 29th Avenue
Eugene, Oregon 97405
541-344-9125
541-344-1481 (fax)
Web Site: http://responsiblenetizen.org
E-mail: info@responsiblenetizen.org

Part II. Safe and Responsible Internet Use Plan

4. Safety and Security of Students When Using Electronic Communications

CIPA Requirements

The CIPA Internet Safety Plan requirements related to electronic communication are:

> (I) IN GENERAL.-- In carrying out its responsibilities under subsection (h), each school ... shall--
>
> (A) adopt and implement an Internet safety policy that addresses-
>
> ...

(ii) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic commerce.[1]

Direct Electronic Communication in Schools

A Sad Story

> A southwest state has a new virtual high school. Coursework for the virtual high school is dependent upon e-mail, but one particular school district in the state is using a filtering system that blocks all e-mail. The kids type their messages and save them to disk, and the teacher takes them home with her and posts from her home e-mail at night. When a reply comes in, or another posting, she prints it out at home and takes it back to students in school the next day. So the teacher is sending the students' e-mail for them since they can't do it themselves. If a different teacher were less willing to help them on her own time, these rural students would be cut off from using virtual school courses. They expect that they will also be unable to use the chat/discussion functions of the online courses as well because chat is also blocked[2].

The use of e-mail and other forms of direct electronic communication for instructional purposes is becoming increasingly important. Some districts have thought the costs and/or the potential dangers cannot be justified. But as the educational use of the Internet matures, this approach will not be sustainable. The Internet is a communication system, in addition to an information system.

It is possible to effectively address the safety and security of students without preventing them from fully participating in valuable educational activities on the Internet. Districts or schools that think they have solved the concerns by blocking access are interfering with student education and exacerbating the concerns presented by the digital divide. These districts or schools are also probably not effectively addressing the education of their students in online safe communication skills that are essential for safe Internet communication at home.

Educational Purpose and Use

Attention must be paid to purposes for which e-mail and other forms of direct electronic communication are being used to support enriching educational activities. In keeping with the educational purpose of the district's Internet system, excessive amount of use for personal purposes should be discouraged. This issue is discussed in the chapter on "Educational Purpose and Use."

Types of Electronic Communication

The primary forms of direct electronic communication that are being used in schools are:

E-mail

E-mail is by far the most prevalent form of direct electronic communication. Through e-mail, students are engaging in conversations with students in other parts of the country and the world.

---

[1] 47 U.S.C. 254 (I)(1)(A)(ii).

[2] Story relayed by Jennifer D. Burke, Program Coordinator, Educational Technology Cooperative Southern Regional Education Board, Atlanta, GA. Personal communication, August 2001.

Students are able to take online distance education classes. Students are also able to communicate with experts in subjects that students are studying.

It is true that in some districts, the use of e-mail has become just another means for students to pass notes to each other. The degree to which this kind of communication is considered acceptable varies from school to school and can generally be managed through the establishment of traffic limits.

"Real time" Communication"

"Real time" communication environments, such as Chat and Instant Messaging allow students to engage in real time communication with other people who are online at the same time. Many online educational services have established environments where students can engage in online chats with authors, scientists, and others. Most online distance education classes make use of "real time" communication environments.

There are also a variety of moderated and unmoderated chat environments available on the Internet. The unmoderated chat environments present the most concerns regarding the potential of coming into contact with a predator. Most of the unmoderated chat environments have little to no educational value. Districts can address concerns of such environments by establishing a list of approved "real time" environments or limiting such activity to approved class activities.

Online Discussion Forums

Online discussion forms or conferences are also used to support distance educational classes, especially when students are participating from different areas of the world. There are also online discussion forums where students from around the world are engaging in ongoing discussions about a wide range of issues of interest or concern to youth. These environments present incredible opportunities for students to expand their understanding of our global society.

The online discussion environments can be managed in the same manner as "real time" communication environments.

Web-based E-mail Services

In some districts, where the district itself has not provided for e-mail, teachers and students who require e-mail for educational activities have utilized the services of commercial web-based e-mail providers, such as Hotmail or Yahoo mail. The use of these systems by students presents significant concerns. These services are provided for free to the user, but the costs are supported by advertising. Lots of advertising. The systems are developing market profiles of their users that may contain both demographic information and interest information collected when a user responds to an advertisement. Many people are using these web-based e-mail systems to transmit pornography, invitations to engage in gambling, and all other manner of unwanted solicitations.

In sum, these services are simply not the kinds of places that districts should be allowing students to use. *However*, districts should never simply dictate that all use of commercial web-based e-mail systems should immediately terminate. If teachers and students are using these services for valuable educational activities alternatives must be put into place prior to any restrictions being placed on the use of the systems.

Some districts simply do not the resources necessary to support a district-based e-mail system. In such a case, there are reasonable alternatives that provide an excellent, safe educational environment for students. Fortunately, the subscription costs for such services are quire reasonable. Any district that cannot afford to maintain its own e-mail system should consider such services as an alternative.

Weblogs

Weblogs or blogs are services offered on the web where students can write and publish their thoughts about a topic. Weblogs are a merger between web sites and group discussions. On traditional web sites, the process of posting information can be laborious. On weblogs, the typing and posting can occur quite rapidly. Many individuals throughout the world are using weblogs to create daily journals. Weblogs offer the ability for others to comment on the posts. Teachers are beginning to use weblogs in a similar manner to the traditional "daily journal." Weblogs encourage writing, discussion, and interaction.

Safety and Security Concerns

There are four areas of greatest concern when students use electronic communication:

- Privacy, which is discussed in Chapter II-6.
- Receipt of unsolicited E-mail (SPAM) e-mail that contains pornographic or other inappropriate material.
- Harassment and bullying of students by other students.
- Engagement with an online predator.

SPAM

SPAM is unsolicited e-mail that can contain a variety of material, ranging from unwanted advertising and get rich schemes and pornography or links to pornographic sites[3]. From safety perspective, the most significant concern is pornographic SPAM[4].

To effectively address concerns related to SPAM requires both a technical solution and an educational solution. SPAM blocking technologies can help to limit, but not totally prevent, the receipt of SPAM. If a school maintains its own e-mail capacities, SPAM blocking technologies should be incorporated into this system. If a district uses an education subscription service, the SPAM blocking technologies will be built into the service.

Staff and students should also be educated about how to deal with SPAM. Here are some of the basics:

---

[3] To understand why such e-mail is called SPAM, one must travel the recesses of Internet memory and watch a Monty Python movie. This has been beyond my grasp.

[4] Educational products companies are sending e-mail messages advertising educational products to teachers--a practice that may or may not be considered SPAM depending on the degree of flexibility in the definition. Whenever a teacher provides personal information at a tradeshow booth at an educational conference, the company now has a valid e-mail address of a potential customer. The degree to which such companies may be using and selling such information may present concerns--as it is not a general practice for such companies to hand out a privacy policy at the time they ask for such personal information.

- Recognize that the more places users leave their e-mail addresses, the more likely it is that they will end up on a spammer's list of e-mail addresses. Spammers use search technologies to "harvest" e-mail addresses from public places on the Internet. The most popular places to harvest e-mail addresses are contest entries, bulletin boards and kid's clubs. Under the educational purpose restrictions, users of a district e-mail system generally should not be engaging in the kinds of uses that would generally lead to registration on commercial web sites or participation on online communication activities that are the primary source of such e-mail addresses. As discussed in Chapter II-6, students should not be encouraged and required to provide personal information, including their e-mail address on sites unless their has been a review of the privacy policy. If any particular users are having difficulties with extensive amounts of SPAM, it may be necessary to determine what activities they are engaging in that are leading to the harvesting of their how their e-mail addresses.

- Users must learn to recognize SPAM prior to opening the message and transfer the4 unopened messages to the trash file. The basic safety requirement is never to open an e-mail message unless you know who the sender is. SPAM is usually pretty easy to recognize. The sender's name is usually disguised, frequently with lots of numbers. The subject lines contain fascinating "enticements," such as: "Make money at home." "You just won." "See my new web site." "A special message for you." "Look at my new girlfriend." When SPAM messages are opened, they can immediately display inappropriate material. These messages that should be immediately transferred to the trash file without opening.

- Users should know that they should generally not respond to the "Remove me from your list" feature that is on some SPAM messages. This feature is generally a scam. If a user responds to a SPAM message requesting removal, this verifies to the spammer that the address is a valid address. They can then place this address on their premium list of verified e-mail addresses. This guidance does not apply to the educational product companies who are generally responsive to such remove requests.

- The receipt of pornographic SPAM or any other sexually explicit e-mail by a student with a K-12 e-mail address should be treated as a criminal matter. The sender of such messages should know, or have reason to know, that sending pornography to a domain would result in providing sexually explicit material to a minor. Such actions are likely to be in violation of both federal and state criminal laws. Successful prosecution of several cases would go a long way to helping pornography spammers to be very careful in their handling of K12 domains.

  Students and staff should be instructed to save any pornographic e-mail message they receive and to immediately notify the building administrator. The administrator should contact one of more of the following:

  - Local FBI office -- Computer Crime or High-Tech Crime unit.
  - US Department of Justice's Child Exploitation & Obscenity Section[5]
  - State Attorney General's office.

[5] URL: http://www.usdoj.gov/criminal/ceos/.

Online Harassment and Bullying

Unfortunately, harassment and bullying that can occur in the "real world" at school can also occur online. Words can hurt and the hurt can lead to very negative consequences -- including school violence and suicide.

As discussed in Chapter III-2, if school staff are aware of harassment or bullying and fail to respond, there is a potential for liability.

Unfortunately, just as students may be reticent to report harassment and bullying that occurs in the "real world," they may be equally reticent to report online harassment. One advantage, however, to online harassment and bullying is tangible evidence in the form of the actual electronic messages. Once a few students have been detected and punished for sending harassing or bullying messages, the existence and impact of the tangible evidence should be well understood by all of the students in the school.

Teachers should naturally be sensitive to their student's emotional demeanor when using the Internet. If a student is looking distraught while using the Internet, this is the time for adult attention to what may be causing such distress. Technical monitoring systems may also be configured to detect patterns of language that give rise to concerns about bullying.

Obviously, this is a situation that must be handled with great care. The student who is the recipient of bullying who has not reported such bullying probably is a fragile child with significant fears. Physical reprisal from the student engaging in the bullying is a strong potential.

Online Predators

Online sexual predators and other potentially dangerous individuals, including cult or hate group recruiters, may communicate with students through the Internet. It is unlikely that students will make significant contacts with online predators when using the Internet in school -- unless the school is providing extensive open access periods with little-to-no supervision, which, of course is not advised. Educational activities that students would be involved with at school do not occur in the kinds of environments where predators tend to "hang out."

Young people are far more likely to make contacts with online predators when they are using their computers at home. It is a big mistake to think that limiting electronic communications at school will address the concerns for what happens at home. Filtering software in school will not address concerns of predators. What might?

- Staff development for teachers so that they are aware of the indicators that a young person may be drifting into a trouble situation.

- Education for parents providing guidance on addressing addiction and predator concerns.

- Education for students about predators, dangerous activities, and the need to tell a responsible adult if you are concerned or if you think a friend is getting into a potentially dangerous situation.

Internet Savvy Teens

It is important for educators to be aware that many teenagers have the online sexual pervert and predation situation pretty well under control. Internet savvy teenagers can recognize perverts and predators for who they are and quickly tell them to "get lost."

Unfortunately, we have not yet taken full advantage to "teen power" to address the concerns of online predation. If more teenagers knew how to recognize, and preserve evidence, and report cases of contact by a possible predator, the ability of legal authorities to identify and prosecute these individuals would greatly increase. Teenagers simply do not know how important this is. Schools can help educate them about the importance.

Additionally, it is highly likely that any student who is thinking about meeting with an individual she (and sometimes he) has met online will share such plans with a friend. Students need to understand the potential dangers and the importance of never meeting with an online stranger outside of the presence of a parent or other adult. Students need to understand the potential consequences to their friends under such circumstances and recognize the need to either dissuade their friend from engaging in such a meeting or, if unsuccessful, to tell an adult.

Students should know that addressing their concern for the safety of their friend does not mean that they should go along with their friend to meet the online stranger. There have been a number of reported incidents where a friend has gone to such a meeting, only to get entrapped by the predator.

Students must learn how to recognize signs of a predator, how to preserve and report evidence, the importance of practicing safe skills, and the importance of watching out for the well-being of their friends. It is critically important that students learn and practice these skills in school.

Addressing Electronic Communication Concerns

The following are strategies that districts should consider implementing to address the safety and security of their students when using electronic communication systems

- For elementary students limit e-mail access to class accounts or systems where the teacher has full and immediate access to all electronic communication. Allow secondary students to have e-mail accounts to support educational activities. Establish the accounts with usernames that will help to protect the student's actual name. Do not simply use the student's last name. Most students will sign their messages with their first name and would thereby reveal their full name.

- For all students, limit the use of "real time" communication activities only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the school. Students should be able to identify and access the approved educational communication environments through the school's web site.

- Place strict limits on the size and level of activity allowed through student e-mail accounts. Students who have an educationally justifiable reason for a greater amount of e-mail use,

such as students in school leadership positions, school newspaper staff, etc. may petition for greater storage and use limits. Indicate to students that excessive e-mail activity that has not been justified may create a reasonable suspicion that the student is misusing his/her e-mail account for personal purposes.

- Do not allow the use of the free, advertiser-supported commercial web-based e-mail services through the district's Internet system. However, prior to putting this restriction in place, ensure that other e-mail services are available.

- Include in the policy several provisions addressing student safety, including communication safety, personal privacy, protecting the privacy of others.

    - Elementary and middle students should not disclose their full name or any other personal contact information for any purpose. High school students should not disclose personal contact information, except to education institutions for educational purposes, companies or other entities for career development purposes, or with specific staff approval. Personal contact information includes the student's full name together with other information that would allow an individual to locate the student, such as parent's name, home address or location, work address or location, or phone number.

    - Students should not disclose names or personal contact information about other students under any circumstances.

    - Students should not agree to meet with someone they have met online without their parent's approval and participation.

    - Students should promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable, especially any e-mail that contains pornography. Students should not delete such messages until instructed to do so by a staff member.

- In the professional development delivered to district staff around the safe and responsible use of the Internet, ensure that teachers are aware of issues related to SPAM, harassment and bullying, and online predation.

- Address issues of online predation in classes for students related to the safe and responsible use of the Internet, as well as sex education classes. Students should be well aware of the very real trauma that other young people have gotten themselves into when they met with an online stranger. Students should also know the signs of predation and when they might be at risk for becoming involved with a predator. Stress the importance of saving and reporting evidence of such interactions as a contribution to the well being of other young people. Also discuss and practice how students can intervene with their friends who may be foolishly thinking of meeting with an online stranger.

- Provide leadership within your community to address all forms of sexual and physical abuse.

- Promptly contact appropriate legal authorities in the event a student has received a pornographic e-mail message or other inappropriate communication.

- Help empower your students, especially your female students, to address victimization in all forms. The National Center for Missing and Exploited Children has an excellent new public awareness campaign for teen girls, *Know The Rules*[6]. Their site has excellent resources for teachers in conjunction with this program.

[6] URL: http://www.ncmec.org.