RIKER
DANZIG
SCHERER
HYLAND
PERRETTI LLP

Technology in the Schools: Legal Implications for Students*

Before the late 1990s, when students got ready to go back to school, parents took their children to the store and bought them pens and paper, highlighters - maybe even a fancy calculator.

This September, when the class of 2001 got ready to go back to school, their parents took them to the store and they bought (along with beepers and cell phones, laptops and home computers. In the twenty-first century, computers have become a staple "back to school" item - both at home and in classrooms around the country.

In 1996, approximately 65% of America's public schools were connected to the Internet. Of those schools with access to the World Wide Web, approximately 75% made web access available to students. By September 1998, 89% of all public schools in the United States had access to the Internet either in classrooms or school libraries.

Computers can be great for students in many ways: they can enhance instruction and research, increase work efficiency and - via the Internet - connect a classroom in Morristown, New Jersey, to classrooms around the globe. Computers can broaden horizons and provide an alternative means of communication for many students.

But the introduction of computers into schools also has risks, and local boards of education must protect students, staff, and themselves from liability.

Boards must take precautions and guard against misuse:

- making sure that users access only appropriate sites on the Internet;
- making sure that users understand the dangers of on-line communication; and
- making sure that networks are reserved for educational purposes.

In addition, boards of education must do all of these things without infringing on privacy and speech protections of the First Amendment.

Role of the Board of Education

Boards of education have ultimate responsibility for overseeing computer network use in schools, ensuring that student use coincides with the specific and limited purpose of enhancing the delivery of education. Further, boards must ensure that students are protected in the virtual world and that parents are fully informed as to how the system is being used by their children.

At the same time, school districts must protect themselves from liability from two potential sources:

(1) liability for negligence when students access inappropriate sites or material when using the school-provided Internet connections - the basis of the lawsuit would not be that the student accessed the inappropriate material, but that the district was negligent and failed to take reasonable precautions against this risk; and

(2) liability when students use the network to cause harm to another person or organization (e.g.: defamation, harassment).

AUPs

To reduce potential liability, boards formulate and adopt Internet User Agreements or Acceptable User Policies (AUPs).

AUPs are sets of rules and regulations that set forth student rights and responsibilities with respect to Internet use through school equipment. AUPs are generally drafted in the form of an agreement, signed by the student and his or her parent or guardian. They should reference the school district's code of conduct, making a violation of the AUP a violation of the code of conduct. The agreement is essentially a permission form to allow student access to the Internet.

The AUP may also satisfy a school board's obligation under N.J.S.A. 18A:35-4.17 to notify students (as part of the district's computer education instruction) on the potential risks and dangers posed to children by persons who use interactive computer services for illegal purposes. In order to satisfy the statute, the AUP must include safe computing guidelines.

The AUP should explain the purpose behind network access and delineate the proper use of the Internet and electronic mail network. At a minimum, it is recommended that the AUP state that:

1. The network must be used exclusively for educational purposes;
2. Users must use educationally appropriate speech and expression when using the network;
3. Users will be expected to adhere to the same standard of conduct expected in the classroom;

4. Users must avoid copyright violations;
5. Users should understand that there is no expectation of privacy in any and all uses of district technology resources;
6. Users must respect the privacy rights of others; and
7. Users must avoid substantial and material disruption of the educational process for the school community.

In addition, the AUP should include a non-exhaustive list of examples of prohibited use. For example:

1. Users may not access, send or display educationally inappropriate materials;
2. Users may not use the network for non-educational purposes;
3. Users may not use profane, obscene, vulgar or abusive language (with those terms defined);
4. Users may not use network systems to harass, insult or attack others;
5. Users may not use the network for commercial (purchasing products online) or for illegal purposes;
6. Users may not use another student's password, or hack into district programs or violate the integrity of district servers; and
7. Users may not damage network equipment. Parents should pay particular attention to this warning in light of N.J.S.A. 18A:37-3 which hold parents liable for a student's damage to school property.

It is critical that students and parents are forewarned about the potential disciplinary consequences for improper use of district equipment. In addition to whatever penalties the law may impose, network use is a privilege which may be revoked if there is a finding that a student has engaged in inappropriate use. Of course, these disciplinary measures are imposed as any other disciplinary measure - with full regard to due process considerations.

In addition to signing the AUP, boards should require parents and legal guardians to sign a release which holds the district harmless for his or her child's unauthorized use of the network at school. Parents and legal guardians must appreciate that it is impossible for schools to oversee the network use of each student at all times - unlike traditional educational materials such as books, filmstrips or even computer software learning programs, the network is impossible to completely censor or control. If parents and guardians chose not to assume this risk, they can elect not to sign the AUP and release.

First Amendment Concerns

One of the toughest questions is the extent to which students enjoy freedom of speech and expression on the Internet, and to what extent they enjoy privacy in their communications. For example, when students post or attempt to view or download information on the Internet or send and receive e-mail messages, can the school district intervene and restrict the communication?

A. Freedom of Speech and Expression.

First, although there is little case law yet on the issue, student speech and expression on a network will likely be treated by courts in the same manner as student speech and expression using other media. Therefore, despite the constitutional protection of expression, public school administrators can, upon a showing of compelling justification, impose reasonable time, place and manner regulations on expression.

At the outset, please remember that there are classifications of speech that are unprotected:

1. Fighting words or speech or expression that presents a clear and present danger of imminent lawless action.

2. Obscenity: Student attempts to post, view or download obscene information, graphics or messages on or from the network is not protected. This, of course, begs the question as to what constitutes obscenity. Using the standard set forth in 1973 by the United States Supreme Court, obscenity is anything that: (a) appeals to a prurient interest in sex; (b) depicts sexual conduct in a patently offensive way; and (c) lacks serious literary, artistic, political or scientific value.

3. Along similar lines, lewd, vulgar or indecent communications may not be protected. If the expression is merely indecent but not strictly obscene, it is protected by the First Amendment - but remember that what is merely indecent for adults is often obscene for children.

4. Disruptive Material: School districts need not tolerate disruptive network communications. Districts can curtail this expression when it "materially or substantially disrupts the smooth functioning of the school or interferes with other students rights." Tinker v. Des Moines Indep. Sch. Community Sch. Dist., 393 U.S. 503 (1969). Therefore, schools may censure "school-sponsored" student speech if it is lewd, indecent or offensive and, therefore, undermines the educational mission of the school.

There are several cases of school districts disciplining students for obscene, vulgar and disruptive speech. For example:

* In an early case of Internet abuse, a California school disciplined 4 students during the 1994-95 school year for attempting to download Playboy Magazine photographs and using vulgar language in a chat room.

* In a South Carolina high school in late 1996, a student put computer viruses on school computers and placed racial epithets about school officials on his World Wide Web site. The student was suspended, then transferred to another school.

* Finally, in a closer case in Texas in 1998, a 13-year old boy was disciplined for seemingly inoffensive speech that

occurred outside of the school setting. The boy drew a picture of a Chihuahua in the school computer lab as a class project. As a spoof, he eventually turned the drawing into the beginning of a Web site he designed on his home computer. The site contained humorous attacks on Chihuahuas and was called "Chihuahua Haters of the World" or CHOW. A Chihuahua breeder came across the site and threatened to stage an animal rights protest if the boy's school failed to take action. The student was removed from his Emerging Technology class at school and suspended for 1 day when he refused to remove the page from the Internet. The student's discipline report noted that he was punished for "creating a Web page implicating a school animal hate group."

5. Threatening speech: In addition to obscene, vulgar or disruptive speech, true threats are not protected by the First Amendment. For example, in 1997 the United States Secret Service released information about an investigation into student on-line death threats against President Clinton - many of the threats were sent on school computers. Also, in 1998, a high school student in Allentown, Pennsylvania was disciplined for using the Internet to post the names of two teachers and two classmates on a list of people who should be shot. These actions are completely unprotected.

District Control Over Network Use & Access

Although school districts can install filtering software and blocking devices, there will always be cries of censorship and there is a question under the law as to whether these devices satisfy the requirement that governmental restrictions on free speech be narrowly tailored. Because the software and these devices rely on recognition of predetermined words or phrases and screens for those words or phrases, there is the potential for the school blocking out appropriate educational material.

Even if the use of these devices is upheld, school districts will still have to justify their determination of what is being filtered or blocked. The analogy would be a school board's decision to ban certain books from the school library. School districts have to review controversial materials and determine their "educational suitability" - they cannot deny student access to ideas or information simply because they are unpopular or simply because the majority of the school board disagrees with them.

There had been a federal act which would have assisted schools and parents in filtering out objectionable sites - it was passed in conjunction with the Telecommunications Act of 1996. Section V of the Telecommunications Act was known as the "Communications Decency Act of 1996" or the CDA. In part, under the CDA, it was a criminal offense to knowingly transmit indecent or patently offensive materials over the Internet to persons under 18 years of age. Although the law would likely have reduced inappropriate transmissions to school-age children, in 1996, the United Stated District Court for the Eastern District of Pennsylvania ruled that those provisions of the CDA were unconstitutional (violating the First Amendment as a content-based restriction on speech) and, in 1997, the United States Supreme Court upheld this ruling. ACLU v. Reno, 117 S.Ct. 2329 (1997).

B. Student Privacy Rights. The second question is whether students enjoy an expectation of privacy in their communications across the school district network. The answer to this question depends on several factors:

> (a) how the district structures Internet services; (b) what the district tells students about their rights to privacy; and (c) the expectations of privacy that relate to specific uses of the Internet (e.g., there is generally a greater expectation of privacy in personal e-mail versus web research).

We can look to the seminal case of N.J. v. T.L.O. for guidance on when a search of a student's on-line files is permissible. Under T.L.O., the search must be justified at its inception (meaning that there are reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school). Second, the search must be "reasonably related in scope to the circumstances which justified the interference in the first place" (meaning that it is not excessively intrusive). These standards are easily applied to student Internet use where there is suspicion of illegal activity or activity violating school rules.

The more difficult question is whether these same standards can be used for random searches through the contents of a student's e-mail files and records of their on-line activities. The answer to that question will depend on whether the student has a reasonable expectation of privacy.

As a general matter, school districts should address this issue in the AUP and advise students and parents that school officials retain the right to view and access any network communication. The AUP should clearly state that there is no expectation of privacy on the network. Apart from student use of school networks, there is an additional question of how much control school districts have over student computer use at home, where there is some connection to the school.

For example, in Beussink v. Woodland R-IV Sch. Dist., 30 F.Supp. 2d 1175 (E.D. Mo. 1998), a high school student was suspended by the school for 10 days for posting a home page on the Internet that contained crude and vulgar language and was also highly critical of the school and its administration. The homepage was created by the student

on his home computer, in his home, outside of school hours. Although there was no documented disturbance at the school as a result of the site, the site did contain a hyperlink allowing readers to access the school's homepage and invited readers to contact the school's principal and voice their own opinions about the school.

The student removed the homepage from the Internet and served the suspension, but the suspension caused the student's grades to drop significantly. The ACLU became involved and brought suit on behalf of the student.

The ACLU won - the court issued a preliminary injunction which prevented the school district from imposing any academic sanctions against the student. The court held that simply disliking or being upset by the content of a student's expression was not an acceptable justification for limiting it. As stated by the court - unpopular speech invites censure and needs the protection of the First Amendment.

In contrast, in Pennsylvania, a teenager was permanently expelled for his web-site titled "Teacher Sux." The site consisted of several pages that made derogatory comments about the student's eighth grade algebra teacher and his middle school principal. The student pictured the teacher with her head severed and dripping blood, and solicited contributions to help him hire a hit man to kill her. The site also morphed the teacher's image into that of Adolf Hitler and called her a "fat bitch." As for the principal, the student accused him of an extramarital affair. The court accepted that the teacher and principal felt both threatened and embarrassed - and noted that users accessed the site 234 times before the student took it down. The court held that the site materially disrupted the learning environment in the school and that the district was justified in expelling him. J.S. v. Bethlehem Area Sch. District, (July 14, 2000).

COPA

As a final matter, school districts should take all measures to guard students from disclosures of personal information in the virtual world.

Although Congress' first attempt at legislation in this arena failed (the Communications Decency Act which was found unconstitutional in 1997), there was a second attempt designed to protect children from "data miners" and from harmful materials, the Children's Online Privacy Protection Act (COPA), which was enacted in October 1998. The statute's purpose was to protect minors from harmful materials, which were identified as harmful when measured against contemporary community standards. Also under COPA, sites which were directed at, or knowingly collected information from, children under 13 years of age were required to take steps to obtain parental consent before collecting, using or disclosing personal information about children.

However, in a decision dated June 22, 2000, the United States Court of Appeals for the Third Circuit heard an appeal from a decision by the United States District Court for the Eastern District of Pennsylvania - the District

Court had issued a preliminary injunction which prevents enforcement of COPA on the grounds that the statute is unconstitutional under the First Amendment. The Third Circuit affirmed, stating that, under the First Amendment, Web publishers cannot be forced to restrict access to their sites based upon the locale of the site visitor - community standards will differ. In its decision, the Third Circuit expressly recognized that current technological limitations prevent harmful material on the Web from being constitutionally restricted, and ended with the hope that, with new technology, regulation may be possible.

Of course, regulation becomes increasingly more difficult as children become savvy at hiding their true age and data miners (and predators) become more savvy at getting children to disclose personal information. Teachers should address these issues with students and the dangers of what might happen to information that they transmit through chatrooms, websites, e-mails or even through "cookies," which store information about a user's preferences.

Conclusion

With new technology comes new responsibilities for school districts. Computer networks open new forums for research and learning, and expand the repertoire of instructional tools for teachers, but computer networks in the hands of students also pose risks. To a great extent, school districts need to control what information students have access to and, more importantly, who has access to student information.

Sources

Legal Aspects of Internet Accessibility and Use in K-12 Public Schools, Drs. Conn and Zirkel, 146 Ed. Law Rep. 1 (Sep. 28, 2000)

Sally Rutherford, Notes and Comments, "Kids Surfing the Net At School: What are the Legal Issues?," 24 Rutgers Computer & Tech. L.J. 417 (1998)

Nancy Willard, "Legal and Ethical Issues Related to the Use of the Internet in K-12 Schools," BYU Educ. & L. J. 225 (2000)

Joseph Mallia, "Internet Safeguarding Concerns Area Schools," The Boston Herald, Feb. 16, 1997, at 12

Philip Pina, "Student Codes of Computer Conduct," USA Today, Nov. 15, 1995, at 7D

Jeff Bean, "Out of Line On-Line," L.A. Times, Aug. 24, 1995, at B1

Gus Venditto, "Safe Computing," Internet World, Sept. 1996, at 49

Leora Harpaz, "Internet Speech and the First Amendment Rights of Public School Students," BYU Educ. & L.J. 123,

124-25 (2000)

Robyn Blumner, "Censoring Students in Cyberspace," St. Petersburg Times, Sept. 13, 1998, at 4D

Evelyn Theiss & Kevin Harter, "Access to Web Lifts Lid From Student Expression," The Plain Dealer, March 21, 1998, at 1B

Jeff Bean, "Out of Line On-Line: District Tightens Policies on Computer Use After Some Students Sneak Into RisquÃ© Web Sites," L.A. Times, Aug. 24, 1995, at 1

Lawrence C. Hall, "Internet Threats Punished," Allentown Morning Call, Sept. 11, 1998, at B1

Bret Jessee, "Student Put Racial Slurs on Web Site," Charleston Daily Mail (S.C.), Dec. 18, 1996. at P40

"Secret Service Investigates Internet Threats," Associated Press, Feb. 22, 1997, available in WL 2503170

Joseph Mallia, "Federal, Local Officials Eye Threats Via State E-mail," The Boston Herald, May 13, 1999, at 6

Joseph Mallia, "Mass. Student Taken to Task for Implied Internet Threats," The Boston Herald, May 14, 1999, at 16

Kenneth J. Cooper, "This Time, Copycat Wave is Broader; Schools Scramble to Respond to Violent Threats Since Littleton," The Washington Post, May 1, 1999, at A6

Tracey Cooper, "Boy's Pet Web Page Spoof Comes Back to Bite Him," The Orange County Register, March 7, 1998, at A11

Patrice Mitchell, "Not Just a Game Anymore," L.A. Times, Jan. 3, 1997, at E1

Statement of Nancy Willard, Director, Center for Responsible Use of Information Technologies, Center for Advanced Technology in Education, University of Oregon, College of Education, presented to, House Commerce Committee, Related to House Resolution 3177, Sept. 16, 1998, available at http://netizen.uoregon.edu

Sidney Sayovitz, President, Association of New Jersey School Attorneys, quoted by, Jeffrey C. Mays, "As E-mail Proliferates, So Do the Rules," The Star-Ledger, Dec. 1=25, 1998, 41

Effective Technology Planning for the Technology Literacy Challenge, available online at: http://netizen.uoregon.edu/documents/policy.html

Intermediate Education Service District and Participating School District Internet Policy, available online at, http://netizen.uoregon.edu/templates/esd_policy.html

Christine A. Amalfe & Kerrie R. Heslin, "Courts Start to Rule on Online Harassment," New Jersey Law Journal, July 10, 2000

Practice:

School Law