

Fall 3-2-2000

Legal and Ethical Issues Related to the Use of the Internet in K-12 Schools

Nancy Willard

Follow this and additional works at: <http://digitalcommons.law.byu.edu/elj>



Part of the [Education Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Nancy Willard, *Legal and Ethical Issues Related to the Use of the Internet in K-12 Schools*, 2000 BYU Educ. & L.J. 225 (2000)
Available at: <http://digitalcommons.law.byu.edu/elj/vol2000/iss2/5>

.

This Symposium Article is brought to you for free and open access by BYU Law Digital Commons. It has been accepted for inclusion in Brigham Young University Education and Law Journal by an authorized administrator of BYU Law Digital Commons. For more information, please contact hunterlawlibrary@byu.edu.

Legal and Ethical Issues Related to the Use of the Internet in K-12 Schools

*Nancy Willard**

I. LIMITED EDUCATIONAL PURPOSE

A. Limited Purpose Systems

When a school district establishes Internet service, the purpose is not merely to provide students and employees with general purpose access to the Internet. The district Internet system has a very specific, limited purpose: to enhance the delivery of education.

When using a limited purpose system, some uses or activities are considered unacceptable not because they are bad activities, but because they are not appropriate on the particular system. District employees have an obligation to use the district system in a manner specified by their employer and to not abuse their use of public resources. Students have an obligation to use the district system in a manner that supports their education, self-improvement, and career development.

There are several important reasons to be concerned about how students approach their use of the Internet in school:

* Nancy Willard, M.S., J.D. is a member of the research staff of the Center for Advanced Technology in Education (CATE) in the College of Education at the University of Oregon. Her program, *The Responsible Netizen*, is providing research, development and educational outreach related to issues around the use of information technologies ethics by young people. The web site for this program is located at: <<http://netizen.uoregon.edu>>. Willard's background includes teaching children presenting behavior problems, legal practice with a focus on intellectual property and computer law, and consulting school districts in technology planning and implementation. Willard is currently conducting a NSF-funded research project to identify how high school students make decisions about legal and ethical behavior in their use of interactive technologies.

By combining legal analysis with practical implementation recommendations, this paper was initially drafted to provide guidance to educators in the development of Internet use policies and practices.

- **Prevention of learning displacement** Educators have precious little time to assist all students in achieving challenging academic standards. When young people are using technology, including the Internet, for activities that are merely entertainment, valuable time and resources are wasted.

- **Appropriate use of taxpayer resources** Taxpayers are supporting the costs of technology in schools because of the promise that technology will assist students in achieving challenging academic standards. Many recent articles and reports criticize increased investments in technology because, in many schools, technological resources are not being used to their greatest educational potential. Schools must recognize that the use of “edutainment” software and use of the Internet for entertainment or shopping does not support the kinds of learning gains that are to be expected through the increased use of technology.

- **Preparation for workplace use** The purpose of education is to prepare students for success in life and work in the twenty-first century. When students enter the work force, they will likely be using their employer’s electronic network that will also be a limited purpose network, with greater limitations than an educational system. An important work skill for students to obtain is self-restraint when using a system in the workplace. Companies should not have to rely on technical blocking systems to ensure that their employees abide by use restrictions. Schools have a responsibility to help educate young people how to self-monitor when they are using a limited purpose system, so that these behaviors may be ingrained by the time the students reach the work place.

- **Prevention of problems with misuse and addiction** There are growing concerns with online addiction—people who spend hours and hours of time in essentially worthless activities. When schools force their students to think about their online activities in the context of the value of that activity to their education and self-

improvement, schools are assisting students in gaining critically important self-monitoring skills that may assist in preventing online addiction.

For all of these reasons, it is highly appropriate for districts to exert control over the use of the district's system and to establish that the system is for a limited educational purpose. If students or employees want greater freedom, they can obtain such freedom by acquiring their own personal accounts through a private provider in their home or through a community technology facility.

B. What is an "Educational Purpose"?

The district or schools must describe what is considered to be "an educational purpose" and outline what activities are considered acceptable and unacceptable on this limited purpose system.

Activities that are generally unacceptable are commercial uses, including purchasing products, and lobbying. Use that is clearly acceptable would include such activities as class assignments and career development activities for students, and professional development and communication activities for employees.

Questions emerge related to activities such as independent web research, independent research or communication through mailing lists and newsgroups, and personal communication. One option would be to restrict student use to specific class-related activities. This, however, would be equivalent to establishing a school library and then telling students that they can only use the library for class assignments.

A better approach is to define "limited educational purpose" to mean "class assignments, career or professional-development activities, and high-quality personal research activities," with the provision that students who require access for class assignments have priority over other uses. A 'real world' analogy that can be communicated to students is that online activities that are equivalent to the kinds of activities that would be generally approved in the school library are acceptable.

The district policy would need to be accompanied by an educational program that assists students in understanding the limitations of a limited purpose system, and in learning how to self-monitor by assessing the purpose and quality of

their activities. Engaging students in dialogue about the purpose and quality of their online activities and requiring them to keep a log of their online activities where they must note what their activities have been and the purpose of these activities, may be effective ways to assist students in gaining self-monitoring skills.

All district users should be reminded that their electronic communications reflect on the district and that they should guide their activities accordingly. One way to emphasize this is to require district employees to establish an e-mail signature that identifies their position with the district and to require students to have a signature that includes the name of the district.

C. Recommendations for Establishing a Limited Purpose System

1. Students

- Students requiring access for class activities should have first priority.
- If computers are available, allow educationally related personal interest research/communication.
- Emphasize the importance of self-monitoring skills as future job skill.
- Establish a mechanism that requires students to record or report on activities and state the purpose of those activities.
- Establish methods of monitoring student use.

2. Staff

- Allow limited amount of personal interest research during training, because this helps to spark interest. After training, establish the expectation that use will be limited

to professional development and educational purposes.

- Prohibit participation in group discussions that are not related to education.
- Allow limited incidental personal communication.
- Require an e-mail signature that identifies the staff member and their position within the district., to serve as a reminder that the staff member is using the Internet in their professional capacity.

II. PRIVACY

A. Search and Seizure

1. Issues to Consider

Districts must consider their approach in light of the privacy interests that students or employees may have in the contents of their personal e-mail files or records of online activities.

- **Expectation of privacy** People are still struggling to hold onto the right of privacy at the same time that technology seems to be removing many vestiges of this important interest.
- **Technical** System administrators and technical services personnel have the ability to access personal files and monitor online use. General system administration does not require that the technical personnel review personal files and most personnel respectfully do not read other people's mail. However, there is always the possibility that during routine maintenance the contents of a student or employee mailbox will be accessed. The system administrator must investigate any unusual activity on their system and will likely be required by the district from time to time to report on the manner in which the district system is being used. These activities also raise the

potential that information about the use of the system by an individual will be discovered.

- **Student monitoring** Instructional staff must carefully monitor students when students are using the Internet because of the possibility that students will access inappropriate materials or engage in inappropriate activity when using the Internet. This will necessarily impinge on the privacy interests of students.

- **Education about privacy** The easiest approach for a district would be to establish a policy that allows for review of personal files at any time. But districts ask students to respect the privacy of others by not posting personal information and not forwarding personal mail they receive without permission. At the very least, it is incongruent to require that the students respect the privacy of others, when the district will not respect their own privacy.

- **Legitimate need for privacy** there are times that students may have a legitimate need for privacy. For example, a student who is dealing with sensitive personal issues can find helpful, and legitimate materials available online to assist him or her in addressing questions or concerns.

2. Student Files

The standards for school officials in conducting a search and seizure in the school setting were enunciated by the Supreme Court in the case of *New Jersey v. T.L.O.*¹ These standards are:

- Was the search “justified at its inception”?² A search is justified when 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

1. 469 U.S. 325 (1985).

2. *Id.* at 341.

school.”³

- Was the search “reasonably related in scope to the circumstances which justified the interference in the first place”?⁴ A search is reasonable when “the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction.”⁵

Clearly, the *T.L.O.* standards would apply in cases where there is an individualized search based upon reasonable suspicion of wrongdoing. The question remains whether the district can randomly investigate the contents of a student’s personal e-mail files and the records of their online activity. The answer to this question depends on whether the student has a reasonable expectation of privacy.⁶

Students’ expectation of privacy related to their Internet use will depend on a number of factors, including how the district has structured the Internet services, what the district has told the students, and the natural expectations that relate to specific uses of the Internet. For example, virtually all people feel that their personal e-mail is and should be considered private. When the district provides individual e-mail accounts to students these accounts will be presumed to be private, absent clear notice to the contrary. However, the expectation that web research on a school system will be private is much less strong. Students generally understand that there is a need for the school to monitor how students are using the web.

District educators will need to balance the interests in protecting privacy against the need for effective monitoring and supervision. The manner in which the district addresses these issues may depend on a variety of factors, including the age of the students and the community environment. Whatever the district decides, it is critically important that students be given clear notice of the standards and expectations.

The following model Internet use policy addresses this issue:

3. *Id.* at 342 (quoting *Terry v. Ohio*, 392 U.S. 1, 20 (1968)).

4. *Id.* at 341.

5. *Id.* at 342 (quoting *Terry v. Ohio*, 392 U.S. 1, 30 (1968)).

6. *Zamora v. Pomeroy*, 639 F.2d 662 (10th Cir. 1981).

You should expect only limited privacy in the contents of your personal files or record of web research activities on the XYZNet. Routine maintenance and monitoring of XYZNet may lead to discovery that you have violated this Policy, the XYZ District disciplinary code, or the law. An individual search will be conducted if there is reasonable suspicion that you have violated this Policy, the XYZ District disciplinary code or the law. Your principal has the right to eliminate any expectation of privacy by providing notice to the students. Your parents have the right to request to see the contents of your e-mail files.⁷

An alternative approach is to make the students fully aware that the record of web research activities is not considered to have any level of privacy. This is especially true if a technical system is used for monitoring. The district should also develop standards regarding who has the right to authorize access or monitoring of an individual student's files or online activities when there is a suspicion of wrongdoing.

There also may be educational or disciplinary reasons for a student's e-mail not to be considered private. The clearest example deals with younger students who use a group e-mail account rather than an individual account. A district, school, or teacher may need to "unprivatize" the personal e-mail of a group of students to achieve certain curricular objectives related to effective communication or as a temporary measure to address widespread communication difficulties. Additionally, "unprivatizing" an individual student's e-mail or records of online activity may be a very appropriate consequence of violating the provisions of the Internet Use Policy. Under such circumstances, clear notice should be provided to students that they should have no expectation of privacy.

3. Staff Files

The extent of a district's ability to investigate the personal files of its employees is less clear. In *O'Connor v. Ortega*,⁸ the Supreme Court held that employees had constitutionally protected privacy interests in the work environment but that the reasonableness of the employee's expectation of privacy must be determined on a case-by-case analysis. The Court then ap-

7. Written by author.

8. 480 U.S. 709 (1987).

plied the *T.L.O.* standards of reasonableness to employer intrusions of employee privacy for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct.⁹

Electronic communications of public employees are generally considered to be discoverable under state public records laws, therefore it could be argued that employees have no expectation of privacy. On the other hand, the common practice is to treat e-mail as private. This could give rise to the reasonable expectation that unless there is a public records request, the district will respect the privacy of an employee's e-mail.

Accessing employee e-mail or records of online activity clearly raises issues of personnel relations. From an effective employee management perspective, the standards under which employees' files are accessed or their activities are monitored should be respectful and fair. A reasonable and prudent approach to this issue would be to rely on the *T.L.O.* standards for searches of both student and employee records with the additional potential for review of an employee e-mail file in the event of a public records request. The fact that a district may have the right to look at an employee's e-mail does not mean that every employee has the right to look at another employee's e-mail. Access of an employee's e-mail is a serious invasion of privacy that should only be undertaken in accord with a strict procedure that requires high level authorization and a written notice setting forth the justification for such access and the results.

B. Privacy on the Internet

Educators must be aware of the need to protect the privacy of students in relation to the use of the Internet. It is important for schools to cultivate respect for privacy and to help students learn how to protect their privacy and that of others when they are using the Internet. Further, the Family Rights and Privacy Act¹⁰ places stringent requirements on school districts related to the release of student information.

There are four basic areas of concern regarding privacy. The first is student information that is placed on the district web site or otherwise distributed through the Internet by

9. *Id.*

10. *See* 20 U.S.C. § 1232(G).

school staff or other students. The second is disclosure of confidential student information by staff via electronic communications. The third is information that a student discloses about himself or herself in e-mail messages or on various web sites. The fourth is school-corporate partnerships that provide the opportunity for companies to gather or solicit personal information from students.

1. Disclosure of Student Information on the School Web Site

Actions that school staff or students may take that would violate the privacy of a student include posting the student's name, class work, or picture on a district web site. Any publication of a student's personal information on the school web site should be considered to fall under the provisions of the Family Rights and Privacy Act.¹¹ The law requires parental notice and consent.¹²

Many schools are responding to this situation by requesting parental consent in a manner that allows the parents different options. Some of the options include: student initials, student first name and last initial, student full name, photo or video of student in group without identification, photo or video with identification, class work without identification, class work with identification, etc. The problem with this approach is practical. School staff cannot be expected to keep track of this amount of individualized information. Inevitably a school will end up posting information not approved of by the student's parents.

A more practical approach would be for the school to determine what student information would be safe, reasonable, and appropriate in accord with the age of the student and the instructional goals. The level of appropriate disclosure will be different at different school levels. Thus, one set of disclosure standards could then be provided to parents with the only option given being that of approving or disapproving the entire set.

At the high school level, the issue of the level of disclosure of student information in student press publications will also

11. *See id.*

12. Schools should also obtain staff consent prior to posting any staff information on the school web site. Staff members may have compelling reasons, such as domestic violence or witness protection concerns, to protect their personal privacy.

have to be given careful consideration. The future of news publications is online. Therefore, there are strong educational reasons to support student journalists in the development of skills for online publications. Addressing this issue requires balancing the interests in privacy of older students against the free speech rights of student press. It is recommended that the standards for high school students be developed to allow for the publication of the full names of students and pictures. Parents would still have the option of disapproving this disclosure.

2. Disclosure of Confidential Student Information

School staff members are generally aware of their legal responsibilities related to the protection of confidential student information. However, problems can emerge in regard to the protection of such information when staff members communicate with each other via e-mail. E-mail tends to be informal. Its use leads to the same kinds of casual conversations that can occur in the staff break room or via telephone. During such casual conversations, confidential student information can be disclosed. But with e-mail, there is now a permanent record of that confidential student information that can be easily disseminated beyond the intended recipient. Staff should be reminded of their responsibilities regarding confidential student information and warned of the potential problems that can emerge due to the nature of electronic communication. One strategy to address this concern may be to develop some type of code to identify such information, for example, the letters "CSI" (Confidential Student Information) could be written into an e-mail message as a signifier to the recipient of the importance of handling the message properly. The requirement to include such an indicator would be a constant reminder to both the writer and the recipient of the importance of protecting privacy.

A student may also violate the privacy of another student by including personal information in an e-mail message. Students have been writing notes and disclosing private information about other students long before the Internet. But there is a vast difference between a piece of paper that is handed to one student and an electronic message that can be sent anywhere. It is important to teach students to respect the privacy of others when communicating electronically and understand the harm that they can cause when they fail to do so. A prohibition

against the distribution of personal information about other students can be included in the district Internet use policy.

3. Student Self-disclosure

Students may disclose personal information in electronic messages or on web sites. Some amount of personal disclosure is to be expected. But the district's Internet use policy should prohibit the disclosure of personal contact information without express permission. Personal contact information includes full name, home address, and parents' names.

The restriction against disclosure of personal contact information may need to be modified at the high school level because some of the ways in which students will be using the Internet will require disclosure, such as providing a university with a name and address to send a college catalogue. High schools may provide permission to disclose contact information in certain kinds of situations.

Another area of concern about student self-disclosure relates to the practices of many of the commercial web sites that target children. Many of these sites are soliciting personal information from children through surveys, contests, and games. These sites use this information to engage in targeted marketing. A recent survey of such sites conducted by the Center for Media Education revealed that 95% collected personal information, 73% had no privacy policies posted, and fewer than 6% had a mechanism established to obtain prior parental consent.¹³ Commercial companies spend a significant amount of money on the development of these sites. They are retaining the services of child psychologists to find ways to make such sites more attractive. Many sites that appear to provide educational activities are really nothing more than commercial "pitches." They are merging education, entertainment, and advertising into "edutainvertising." Such sites present significant concerns for schools because they are very attractive to children and they come disguised as presenting material of educational value.

In 1998, the U.S. Congress enacted the Children's Online

13. *Many Kid's Websites Continuing to Collect Personal Information Without Initial Parental Permission, New Survey Shows*, (last modified July 19, 1999) <<http://www.cme.org/Index.html>>.

Privacy Act,¹⁴ which authorized the Federal Trade Commission (FTC) to develop rules that would place restrictions on companies who solicit personal information from children under the age of thirteen. The FTC has developed regulations to implement this Act.

4. Corporate Gathering of Student Personal Information

A rapidly emerging business model seeks to take advantage of the lack of sufficient resources for technology in schools as an opportunity for companies to gain greater access to students for the purposes of marketing and gathering market research data. Companies are offering free equipment or technology resources in exchange for the opportunity to present advertisements to students and to track student use of the Internet. Information about student use can then be used to guide marketing programs for companies selling products to young people or to individually target students with information about products that might match their personal interests.

While there are strict requirements for parental disclosure and consent placed on academic researchers who wish to gather data from students, there are currently no requirements for commercially-related research. Legislation is pending in Congress that would require schools to disclose to parents any agreement that would allow companies to gather data from students and to receive parental consent prior to such gathering.¹⁵

Regardless of the outcome of such legislative efforts, it is highly recommended that school districts be exceptionally careful when considering such arrangements and ensure that parental notification and consent is obtained.

5. Recommendations For Educating Parents and Students About Internet Privacy Issues

Schools can help educate students and parents about privacy on the Internet in the following ways

- Include a provision in the school Internet policy against student disclosure of personal contact information without express permission or only allow disclosure in identified

14. Children's Online Privacy Act of 1998, 15 U.S.C. §§ 6501-6506(1999).

15. 106th Congress H.R. 2915.

situations.

- Educate students and parents about how to protect personal safety on the Internet.
- Avoid the use of “edutainment” sites in school except to educate about how such sites are being designed to market products
- Teach kids about the need to protect their personal information and how to recognize the “privacy traps” set by the companies
- Teach parents about exploitive practices of commercial sites.
- The Center for Media Education¹⁶ has excellent resources for student and parent education. The National Center for Missing and Exploited Children has excellent materials on child safety on the Internet.¹⁷

III. DISTRICT LIABILITY

A. Is There Statutory Immunity for District Negligence?

Although there are no cases directly on point, it is probable that schools will enjoy federal immunity from liability if a student accesses material placed on the Internet by a third party. This immunity was established through Section 230(c) of the Communications Decency Act of 1996.¹⁸ Other sections of the Communications Decency Act were ruled unconstitutional. However, this section remains in force and has been upheld in a number of court cases.

16. *See supra* note 14.

17. *The Center for Missing and Exploited Children*, (visited May 15, 2000) <<http://www.ncmec.org>>.

18. 47 U.S.C. § 230(c) (1999).

Section 230(c)(1) provides: "(1) Treatment of Publisher or Speaker- No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."¹⁹

As to whether an education institution offering Internet access to its students is an "interactive computer service," the question is directly addressed by § 230(f)(2):

The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.²⁰

§ 230(e)(3) provides: "(3) State Law- Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."²¹

In sum, § 230(c)(1) provides that an "interactive computer service" is not to be treated the same as a content provider; § 230(f)(2) provides that an education institution offering Internet access is an interactive computer service; and § 230(e)(3) provides that inconsistent state laws may not be used as a basis of liability.

The word "immunity" is not in the statute itself. But in *Zeran v. America Online, Inc.*²² the Fourth Circuit Court of Appeals expressly held that "[b]y its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating from a third-party user of the service."²³

In a recent case, *Kathleen R. v. City of Livermore*,²⁴ a mother of a teenage boy sued the library because her son had accessed sexually explicit pictures through the library's Internet service. The City made two arguments based on § 230. The first argument was that § 230 provides federal immunity from liability to service providers for the speech of third-party con-

19. 47 U.S.C. § 230(c)(1) (1999).

20. 47 U.S.C. § 230(f)(2) (1999).

21. 47 U.S.C. § 230(e)(3) (1999).

22. 129 F.3d 327 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998).

23. *Id.* at 330.

24. V-015266-4 (Cal. Sup. Ct. Oct. 21, 1998).

tent providers. The second argument was that in enacting § 230, Congress preempted any state law that may be contrary to § 230. The action was dismissed.

What remains in question is whether a parent could successfully establish a negligence action against a school for harm caused to students due to access to material through the district system. Clearly, a school has a higher duty of care to protect children than does a public library. This question has not been addressed.

B. Negligence Cause of Action

The elements of a cause of action for negligence are determined by state law, which varies from state to state. The common elements are:

- **Duty of care** A district that is providing Internet access will have a duty of care. If the district provides dial-up access and makes it clear that parents are responsible for monitoring home use it would not likely be considered to have a duty of care for activities that occur in the home.

- **Foreseeable risk of harm** Depending on the facts of a case, it is possible that it could successfully be argued that there was a foreseeable risk that students might access material that would be considered inappropriate. However, whether accessing inappropriate material would constitute a risk of "harm" would be a question for further research.

- **Negligence** Negligence is the failure to take reasonable precautions against a foreseeable risk. If there is a foreseeable risk of harm, then a district has an obligation to take reasonable precautions against it. As will be discussed below, this is the area where a district can take affirmative actions to avoid liability.

- **Causation** This element inquires into whether the district's actions or failure to take actions causes the harm to occur. Frequently the question is phrased, "But for the district's actions, would this harm have occurred?" In many cases relating to student use of the Internet, there will likely be student action as a causative factor.

• **Injury or harm** A compensable injury must be a direct consequence of the district's negligence. It would likely be difficult for a parent to prove that his or her fourteen year old son suffered a compensable injury when he violated the school's Internet policy and downloaded pornography. On the other hand, a first grader who inadvertently wanders into a violence site could suffer compensable emotional distress. A student who gets involved with an online predator or who downloads recipes for bombs could also sustain a compensable injury.

The critical legal question in the event of problems arising from Internet use will be whether the district had exercised reasonable precautions against a foreseeable risk. The steps that a district can take to reduce the potential of liability are those that relate to the exercise of reasonable precautions. These are activities that a conscientious district would undertake regardless of concern about liability. Reasonable precautions could include:

- Restrictions in the district's Internet policy addressing personal safety and downloading harmful material.
- Provision of information to parents about the potential dangers prior to their approval of their child's access.
- Ongoing provision of safety information to parents.
- Ongoing instruction to students about personal safety and responsible use.
- Professional development for teachers regarding potential dangers.
- Adequate monitoring of student use of the Internet.
- Affirmative action taken by district staff, if questions or concerns arise.

Filtering software *may* prevent access to dangerous infor-

mation. Filtering software may also be somewhat effective in dealing with online predators if the software is used to block access to chat rooms, which are a primary location for predators.

Under 47 U.S.C. § 230(c)(2), an Internet service provider cannot be held liable on account of:

(A) any action voluntarily taken in good faith to restrict access to or the availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (b) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).²⁵

This provision has not been tested in a case involving student access to inappropriate material through a filtered school system. Under the terms of the statute, an educational institution cannot be held liable for their decision to restrict access. The language does not appear to address situations where a school system has made the decision to use filtering but has failed to use other reasonable precautions and the filtering system failed to block access.

The biggest danger presented by the installation of filtering software is the false sense of security and complacency that may result from such a decision. Educators who do not recognize the limitations of filtering software may falsely assume that the software will alleviate all possible areas of concern. This false assumption could result in the failure to take other reasonable precautions.

Given deficiencies of filtering technology, the constitutional concerns about its use, and the potential detrimental effects of false security, at this point in time it is probable that filtering is a reasonable precaution, but not a *legally required* reasonable precaution.

C. Liability for the Actions of Staff or Students

The potential of district liability if a user causes harm to another person or organization through the use of the district system is a concern. Areas of concern include: defamation, harassment, or invasion of privacy, copyright infringement and

25. 47 U.S.C. § 230(c)(2) (1999).

computer security violations.

1. Defamation, Harassment, or Invasion of Privacy

Section 230 of the Communications Decency Act provides immunity for “interactive computer service” providers for material that is transmitted through their system, but not for “information content providers.”²⁶ Education institutions are included in the definition of interactive computer service provider, but this designation only addresses situations where the district has no control or supervisory responsibilities related to the material transmitted through the system. If the district establishes a district web site, the district is also an information content provider and can be held to publisher standards for any defamatory material posted on the site. Additionally, the district can also be held liable for harm caused by material that is considered to be harassment or an invasion of privacy.

It is possible that districts could be held liable for harm caused by material transmitted through the system by students due to a lack of adequate supervision. But it is also possible that the immunity provided by Section 230 would apply in such a case. The district can be held liable for harm caused by material transmitted by staff.²⁷

2. Copyright Infringement

The district may be held liable for the presence of any material that is posted on the district web site in violation of copyright laws. The “Online Copyright Infringement Liability Limitation Act”²⁸ provides interactive service providers with an exemption from monetary damages for copyright infringement, but only if the provider is not directly involved with the placement of the material. On virtually all school web sites, school staff is or should be directly involved with the placement of the material. If the district is acting as an Internet Service Provider (ISP) and allowing staff, students, student organizations, and/or others to establish personal or organizational web pages without any district-level control, then the district may meet the criteria of the Act. In such cases, there are strict procedures

26. 47 U.S.C. § 230(c).

27. *See id.*

28. 17 U.S.C. § 512 (1999).

that must be followed to avoid liability, including filing with the Copyright Office and placing a notice on the web site.²⁹ However, to meet the criteria of the Act essentially means that the district does not or will not exert any control over the materials placed on the web site. It is unlikely that most districts will think that such a hands-off approach is advisable. Additionally, if such a hand-off approach is used, it is likely that the district will find that it has established a public forum, which would eliminate its ability to exercise any form of control over the "speech" presented on the web site.³⁰

3. Recommendations

The following are actions that the district can take to limit liability to others for the actions of staff or students.

- Establish a process to ensure all materials on a district web site are closely evaluated.
- Provide professional development for teachers and instruction to students about defamation, invasion of privacy, harassment, and copyright law.
- Include an immunity provision in the policy.
- Take *prompt* action if accusations are made.
- Be prepared to stand up for staff or students if false accusations are made.

D. District Liability for Damage to Student

An area of potential liability is a district's failure to protect a student's constitutional rights. If a student's rights, as addressed in this document, are not adequately protected by a district and the student suffers harm as a consequence, the district could be held liable. Potential areas of concern are related to due process, search and seizure, and free speech.

Recently, a number of districts have encountered difficul-

29. See 17 U.S.C. § 512(c)(2) (199).

30. See *infra* Part IV.

ties for inappropriately disciplining students for material that the students have posted on their personal web sites. A district in Ohio paid \$30,000 to settle a case that was filed against them for suspending a student because of material he posted on his personal web site that was critical of his band teacher. In *Beussink v. Woodland R-IV School District*³¹ the court ruled in a preliminary injunction that the school could not discipline the student for material on a personal web page that was very critical of the administration of his school. These cases are discussed more fully in the *Free Speech—Student Speech* section.³²

E. Other Liability Issues

1. Losses Caused by System Failure

There is a potential for a district to be held responsible for losses sustained by users as a result of a system failure. These losses could involve loss of data, an interruption of services, or reliance on the accuracy of information maintained on the district system or accessed through the system. The use of a disclaimer that provides notice of the potential for such loss and disclaims district responsibility should protect the district from liability. Users should also be advised to make a personal backup of material contained on the district system.

2. Unauthorized Purchases

Districts should be concerned about the potential that a user will violate the district restriction against purchasing products or services through the system. The district will want to make it clear to parents that there is a potential for students to use the system in such a manner. The district will also want to include in its policy a disclaimer for any financial obligations arising from unauthorized use of the system for the purchase of products or services.

3. Damage to District System

Another area of concern is damage to the districts system by misuse of the system that causes damage to the system. For example, if a student intentionally places a virus on the sys-

31. 30 F. Supp. 2d 1175 (E.D. Mo. 1998).

32. See *infra* Part IV.

tem, causing the system to fail. This is no different than any other damage caused by a student or staff member and is likely covered in other district policies related to damage to district facilities.

IV. FREE SPEECH: STUDENT SPEECH

It can hardly be argued that either students or teachers shed their constitutional rights to freedom of speech or expression [on the school district's onramp to the Information Superhighway].³³

The issue of students' rights to free speech in the material transmitted through the Internet will arise in a number of ways:

- Student speech in public, discussion group messages.
- Student speech in private e-mail messages.
- Student speech posted on a district web site, including material posted in classroom sections, and the school newspaper. Also, if allowed by the district, material posted on an individual student web page or on an extracurricular organization web page.
- Student speech posted on another web site that has been accessed through the district system.
- Student speech that pertains to the school, teachers, or other students and that appears on a personal web site.

A. Legal Analysis

There have been a number of Supreme Court cases addressing student's First Amendment speech rights. Two of these cases provide the greatest guidance for educators in addressing issues of student speech on the Internet. The earliest case is *Tinker v. Des Moines Independent Community School District*, and the more recent case is *Hazelwood School District v.*

33. *Tinker v. Des Moines Indep. Community Sch. Dist.*, 393 U.S. 503, 506 (1969).

Kuhlmeier.³⁴

1. *What is the Forum?*

Traditional analysis of free speech issues starts with an analysis of the vehicle or “forum” through which the speech is being expressed. The Court in *Hazelwood* explained as follows:

School facilities may be deemed to be public forums only if school authorities have ‘by policy or practice’ opened those facilities ‘for indiscriminate use by the general public, or by some segment of the public, such as student organizations.’ If the facilities have instead been reserved for other intended purposes, ‘communicative or otherwise,’ then no public forum has been created, and school officials may impose reasonable restrictions of the speech of students, teachers, and other members of the school community.³⁵

Since the district’s Internet system has been established for an educational purpose, it should be considered a limited forum, similar to a school publication where the school has maintained editorial control. This conclusion is strengthened by the fact that every user of the district system will be identified by the district domain name that appears in their address and, therefore, all speech that originates from the district system, even private messages, will bear the imprimatur of the district.

However, districts that fail to clearly define the educational purpose of their Internet service and establish a practice of allowing their students to indiscriminately use the system in a manner similar to general public Internet access may find that they have established a public forum for their students. In such cases the ability of the district to govern student speech may be more limited. Student speech that occurs on personal web sites clearly would be considered speech that occurs in a public forum.

2. *Student Speech Involving the District System*

Hazelwood provides the greatest guidance for matters pertaining to student speech that is accomplished using district technology facilities. *Hazelwood* involved a principal’s decision to remove several articles from publication in the school news-

34. 484 U.S. 260 (1988).

35. *Id.* at 267 (citations omitted).

paper. The Court found that the school newspaper was not a public forum because the school did not intend to open the paper to indiscriminate use by the students.³⁶ Because, the newspaper was not a public forum, the Court sought to craft a standard for the application of the First Amendment in "school-sponsored publications, theatrical productions, and other expressive activities that students, parents, and members of the public might reasonably perceive to bear the imprimatur of the school."³⁷ The standard expressed by the Court was:

Educators are entitled to exercise greater control over [activities that may be characterized as part of the school curriculum] to assure that participants learn whatever lessons the activity is designed to teach, that readers or listeners are not exposed to material that may be inappropriate for their level of maturity, and that the views of the individual speakers are not erroneously attributed to the school. Hence a school may . . . 'disassociate itself' not only from speech that would "substantially interfere with [its] work . . . or impinge upon the rights of other students," but also from speech that is, for example, ungrammatical, poorly written, inadequately researched, biased or prejudiced, vulgar or profane, or unsuitable for immature audiences. A school must be able to set high standards for the student speech that is disseminated under its auspices.³⁸

The educationally-based restrictions that would appear to be appropriate for a district to impose include:

- **Criminal speech and speech in the course of committing a crime** Including threats to the President, instructions on breaking into computer systems, child pornography, drug dealing, the purchase of alcohol, gang activities, etc.
- **Speech that is inappropriate in an educational setting or violates district rules necessary to maintain a quality educational environment** Including:

--- **Inappropriate language** Obscene, profane, lewd,

36. *See id.* at 270.

37. *Id.* at 271.

38. *Id.* at 271-72 (citations omitted).

vulgar, rude, disrespectful, threatening, or inflammatory language; harassment; personal attacks, including prejudicial or discriminatory attacks; or false or defamatory material about a person or organization.

--- **Dangerous information** Information that if acted upon could cause damage or present a danger of disruption.

--- **Violations of privacy** Revealing personal information about others.

--- **Abuse of resources** Chain letters, "spamming," and appropriate use of district group distribution lists.

--- **Copyright infringement or plagiarism**

--- **Violations of personal safety** Revealing personal contact information or engaging in communication that could place the student in personal danger.

--- **Educationally-relevant restrictions** The district may also require that student publications meet a variety of standards related to adequacy of research, spelling and grammar, and appropriateness of material (such as restriction of student web pages to school and career preparation activities).

It is also important to understand that public officials cannot limit speech based on viewpoint discrimination. *Hazelwood* did not address this issue directly, but the restriction against viewpoint discrimination is a long-standing First Amendment standard. One of the core functions of free speech is to invite dispute. For example, in *Terminiello v. City of Chicago*³⁹ the Court states: "It may indeed serve its highest purpose when it induces a condition of unrest, creates dissatisfaction with conditions as they are, or even stirs people to anger. Speech is often provocative and challenging."⁴⁰ *There is no suggestion in*

39. 337 U.S. 1 (1949).

40. *Id.* at 4.

Hazelwood that the Court was opening the door for school officials to exercise control of student speech based on their disagreement with the opinions being expressed. Indeed this has been the holding of several Circuit Court opinions interpreting *Hazelwood*.⁴¹

3. Student Speech on Personal Web Sites or Through Personal E-mail Systems

The *Tinker* case⁴² provides the legal standards that should be applied to incidents involving student speech that is not made using school technology facilities but does involve comments made about the school, teachers, or other students. In *Tinker*, school officials had disciplined students for wearing black arm bands to protest the war in Vietnam. The standard established in *Tinker* was:

In order for the State in the person of school officials to justify prohibition of a particular expression of opinion, it must be able to show that its action was caused by something more than a desire to avoid the discomfort and unpleasantness that always accompany an unpopular viewpoint. Certainly where there is no finding and no showing that engaging in the forbidden conduct would 'materially and substantially interfere with the requirements of appropriate discipline in the operation of the school,' the prohibition can not be sustained.⁴³

Subsequent court cases that addressed student underground publications have applied the *Tinker* standard to such publications.⁴⁴ There is limited difference between personal web sites and underground publications.

Recently a court addressed the issue of a district's ability to discipline a student for material posted on the student's personal (non-school) web site in *Beussink v. Woodland R-IV School District*.⁴⁵ In *Beussink*, a high school student posted material on a personal web page that was very critical of the administration of his school. In a preliminary injunction, the court indicated that if the speech had been sponsored by the school, the standard that would apply would have been that of

41. See *Searcey v Harris*, 888 F.2d 1314 (1989) (restriction of a peace organization to participate in a high school career day was a violation of the First Amendment).

42. *Tinker v. Des Moines Indep. Community Sch. Dist.*, 393 U.S. 503 (1969).

43. *Id.* at 509.

44. See *Thomas v. Board of Education* 607 F.2d 1043, 1051 (2nd Cir. 1979).

45. 30 F. Supp. 2d 1175 (E.D. Mo. 1998).

Hazelwood. However, in the *Beussink* case the speech was not school sponsored and therefore the standard set forth in *Tinker* was the appropriate standard to apply. Applying the *Tinker* standard, the court concluded that “while speech may be limited based on a fear of disruption, that fear must be reasonable and not an undifferentiated fear of disturbance”⁴⁶ and that “(d)isliking or being upset by the content of a student’s speech is not an acceptable justification for limiting student speech.”⁴⁷

4. *Extracurricular Organizations*

An analysis of student speech rights must include another area of potential concern—the use of the district Internet system by student extracurricular organizations. Under the Equal Access Act,⁴⁸ districts that allow extracurricular organizations may not discriminate on the basis of religious or political views in the creation of these organizations. This Act, which was enacted at the behest of conservative religious groups, is now providing the basis for the creation of a wide variety of student organizations reflecting a range of interests that may not have been anticipated by the Act’s original champions.

The language of the Equal Access Act relates only to school meetings, but it is highly likely that student organizations will wish to use the district’s Internet system to communicate with their members and others. If the district allows one organization to access the district’s system, it will need to let them all have access. There are a number of benefits to this activity. The Internet can provide an effective way for organizations to communicate and maintaining a web page is a good teamwork based learning experience for the students.

On the other hand, the presence of student organization information on the district web site may create the perception of district sponsorship of controversial or religious activities. Such sites could also get out of hand by providing or pointing to material that could create a fair amount of controversy in the community.

There appear to be three options for a district in this situation:

46. *Id.* at 1180.

47. *Id.*

48. 20 U.S.C. § 4071 (1999).

- Establish viewpoint neutral standards for the web pages that may reduce the presence of controversial material (e.g. require that the material must relate specifically to organization activities and programs; only student-produced material may be posted).
- Allow no web pages for extracurricular organizations.
- Apply no restrictions other than the district communication rules and school rules to the web site. The district will likely want to require that the extracurricular web pages include a statement of the district's neutrality on the views expressed.

Districts that provide few restrictions on student or extracurricular web pages should be prepared to support the free speech rights of its students if questions arise in the community. Controversy can be limited if the district has deliberated about this issue and is ready to respond to any questions that might arise with a clear statement of the value of free speech to a free society.

V. FREE SPEECH: EMPLOYEE SPEECH

A. *Expression of Viewpoint*

If a teacher disagrees with a policy enunciated by the principal, should that teacher be able to discuss their disagreement with the policy in an e-mail message to site council members?

The basic standard for determining whether a district can govern employee speech was set forth in *Connick v. Myers*.⁴⁹ In this case, which involved a non-school-sponsored forum for speech, the Court established a two-step process for determining whether employee speech is entitled to constitutional protection. First, it must be determined whether the speech pertains to a "matter of public concern."⁵⁰ Second, if it is a matter of public concern, it must be determined that the interests of the teacher in speaking as a citizen outweigh the state's inter-

49. 461 U.S. 138 (1983).

50. *Id.* at 142.

est in promoting efficiency in the delivery of educational services in the schools.”⁵¹

Unfortunately, this standard is rather difficult to apply. Not surprisingly, courts have been sharply divided over what constitutes a public concern in the context of speech by teachers and other district employees. Translating the *Connick* standard into a clearly understandable policy for employees presents an even greater challenge.

An additional factor that must be considered is the potential impact of *Hazelwood*. While the *Hazelwood* case did not involve employee speech, it did involve a school-sponsored vehicle for the delivery of speech and, as noted above the, court stated, “If the facilities have instead been reserved for other intended purposes, ‘communication or otherwise,’ then no public forum has been created, and school officials may impose reasonable restrictions of the speech of students, *teachers, and other members of the school community.*”⁵²

Employee speech through a district network will bear the imprimatur of the district, because of the domain name which will be part of the employee’s address. Clearly, the district should have the right to impose the same educationally-based restrictions on employee speech as it does for its students. But does the fact that the district has provided the vehicle for expression and employee speech, and such speech will reflect on the district, entitle the district to also control the content of employee speech?

An argument could be made that when a district employee is communicating through a district-provided system, the district has a legitimate right to govern the content of the employee’s speech. This is basically the same situation that any other employee of a business who is communicating through their employer’s system would face.

On the other hand, the courts have tended to grant public employees greater freedom of speech than private sector employees. We want our public employees to speak out on matters of public concern because this will assist the public in gaining a better understanding of issues related to government activities. If a district believes that our society and our educational system will be benefited by a robust exchange of ideas and opin-

51. *Id.* at 142-46.

52. *Id.* at 267 (citations omitted) (emphasis added).

ions, the district will likely want to support their employees' right to use the district system to express their opinions, even if the district may disagree with the opinions expressed.

What matters most is that the expression of opinion is done in a manner that works effectively to address issues, rather than to cause harm. Districts can best address this issue through awareness and professional development. The district's e-mail system will make public those discussions which, before now, only occurred in the staff lounge. Requiring district employees to use a signature that identifies their position within the district will reinforce the importance of speaking responsibly. Many individuals, particularly those not in leadership positions, have not had the opportunity to learn techniques of effective communication, particularly when dealing with potentially controversial issues. This will be an essential skill for educators as we continue to shift to technology-supported site-based management. This skill can be enhanced through professional development in effective communication.

B. Optional Perspectives:

- The district has the legitimate right to control the content and viewpoints of employee speech.
- Society and district will benefit from a robust exchange of ideas and opinions. Further, employee expression of their personal viewpoint is essential to school reform.

C. Recommendations

- Make it clear that employees are writing in their professional capacity and should guide their writing accordingly.
- Require the use of e-mail signature stating name and district position.
- Establish the standard that writing in professional capacity may include expression of personal professional viewpoint, even if that viewpoint differs from district

position. However, the viewpoint must be expressed in a professional manner.

- Provide staff development in effective communication, especially related to communication of controversial issues.

VI. FREE SPEECH: STUDENT ACCESS TO INFORMATION

Q: How is the Internet like the school library?

A: It opens the door to a world of knowledge

Q: How is the Internet not like the library?

A: No library book selection committee

A. Legal Analysis

The leading case addressing a student's right to access information is *Board of Educ. Island Trees Union Free Sch. Dist. No 26 v Pico*.⁵³ The case involved a school board's decision to remove some books from the school library after receiving a list of "objectionable" books from a politically conservative organization. The court's ruling must be read in light of the facts of the case—the actions of the board were obviously politically motivated, the decision affected the removal of books that had already been acquired, and the books were present in a library and were optional, not compulsory, reading. In this context, the Court stated:

[T]he state may not, consistent with the spirit of the First Amendment, contract the spectrum of available knowledge. In keeping with this principle, we have held that in a variety of contexts the Constitution protects the right to receive information and ideas. . . . [J]ust as access to ideas makes it possible for citizens generally to exercise their rights of free speech and press in a meaningful manner, such access prepares students for active participation in the pluralistic, often contentious society in which they will soon be adult members. . . . [S]tudents must always be free to inquire, to study and to

53. 457 U.S. 853 (1982).

evaluate, to gain new maturity and understanding. The school library is the principle locus of such freedom. . . . In the school library, a student can literally explore the unknown, and discover areas of interest and thought not covered by the prescribed curriculum.⁵⁴

The Court stated that it did not deny that the school board had a "substantial legitimate role to play in the determination of school library content, but that if the intent of the board was to deny access to ideas with which the board disagreed, removal of material was inappropriate."⁵⁵ The message of *Pico* is that it is appropriate for education officials to exercise good faith educational judgment in the selection of materials, but not to attempt to suppress unpopular ideas.

Is *Pico* directly applicable to student's use of the Internet? On one hand, the language of the Court certainly makes a strong case for this. For example, try substituting the word "Internet" for the word "library" in the above passage. On the other hand, there is a clear difference in the manner in which materials are selected for use in a school library by professional educators acting under guidelines established by the board and the manner in which materials are made available on the Internet.

Trying to translate the standards for textbook or library book selection into a provision in an Internet Use Policy that will clearly convey to students where the boundaries for acceptable access are will likely present substantial difficulties. Thus, the challenge for districts is to develop a standard for access that is based on educational judgment, not a desire to suppress unpopular ideas, and that [also] provides clear guidance to students about what they are and are not [permitted] to access.

B. District Policy on Access

Most districts will include provisions in their policy restricting access to material that is profane or obscene (pornography), advocates or condones the commission of unlawful acts (illegal) or that advocates or condones violence or discrimination toward other people (hate literature). However, there may be times when in the context of legitimate research the above restric-

54. *Id.* at 866-96 (citations omitted).

55. *Id.* at 869.

tions are too limited. For example, there may be circumstances where, with appropriate teacher guidance and parental approval, students should be allowed to investigate hate literature sites so that they become better prepared to recognize hate literature and deal effectively with it.

The district cannot be expected to enforce a wide range of family or social values in the kinds of material that students should be allowed to access. The district should provide every parent with information about the district policies and provide an option for parents to request that their child not be allowed access through the district system. Providing students with access to the Internet presents an excellent opportunity to encourage parents to have a discussion with their child about their family values and what their expectations are for their child's activities on the Internet.

The district will also want to include a process for students to follow if they inadvertently access material that is prohibited. This will protect a student from being inappropriately disciplined. If students have dial-up access from home, parents will need to bear the responsibility to monitor their student's actions.

There are many materials on the Internet that would not fall within the "inappropriate material" restrictions of an Internet use policy that would still be inappropriate in school because they are not educationally relevant. Restrictions against inappropriate material covers that material which should, because of its very nature, never be accessed. A violation of this restriction should be treated as a policy violation. Other material should not be accessed because it has no educational value. This issue probably does not rise to the level of a policy violation unless there are repeated incidents of accessing material that is clearly not of educational value. Admittedly, there are many aspects of this issue that fall within a very murky gray zone.

The best defense is a good offense. Teachers who are well prepared to incorporate the use of the Internet into their curriculum and who provide exciting Internet-based learning opportunities will focus their student's attention on all of the wonderfully-positive resources available through the Internet. When all of the computers in the computer lab are kept busy with students doing exciting class work projects, the opportunity for misuse is substantially reduced. Students should not be

provided with access to the Internet until their teachers are prepared to competently guide their Internet exploration activities. Districts that fail to provide sufficient professional development opportunities for their teachers, including the time necessary to incorporate the use of Internet resources into instruction, are the ones that will have more problems with students accessing inappropriate material.

C. Filtering Software

Many school districts are choosing to install filtering software as a strategy to restrict access to material that is considered inappropriate. Filtering software does an adequate job of reducing the potential for inadvertent access to inappropriate material. Filtering software will slow down a teenager who is intentionally seeking inappropriate material, making the activity more of a challenge. However, schools that choose not to install filtering software but which have good policies, exciting educational uses of the Internet, and effective monitoring generally report that they do not have problems with students intentionally trying to access inappropriate material.

Reliance on filtering software does not prepare a young person for the inevitable time that he or she will have unsupervised and unfiltered access to the Internet. Schools that rely on filtering frequently do not address the search skills that young people can use to avoid inadvertently accessing this kind of material, nor do they discuss issues around the darkside of the Internet and the need to make responsible choices. Schools that rely on filtering can become complacent about monitoring, thus leading to other problems. Sometimes the choice to install filtering reflects inadequate dedication to professional development for teachers.

There are potential constitutional problems related to the installation of filtering. There are no cases that directly address this issue. The *Pico*⁵⁶ case, and a recent case involving a public library, *Loudoun v. Board of Trustees of the Loudoun County Library*⁵⁷ provide a basis for analysis.

In *Loudoun*, the court found that the library had "entrusted all preliminary blocking decisions—and by default, the over-

56. Board of Educ. Island Trees Union Free Sch. Dist. No. 26 v. Pico, 457 U.S. 853 (1982).

57. 24 F. Supp. 2d 522 (E.D. Va. 1998).

whelming majority of final decisions—to a private vendor”⁵⁸ that “has refused to provide the criteria it uses to block sites”⁵⁹ and whose blocking decisions are not based on “any legal definition of obscenity or even the parameters of the (library’s) policy.” This delegation, the court determined, was impermissible.

There are no cases on point related to filtering in schools. However, in the case of *Pico*, the Court was especially concerned that the list of “books that should be banned” had been provided to the board members by a conservative political organization. The Court reaffirmed the right of the board and school officials to make decisions about materials to provide to students. In fact, the principal objection set forth in the dissenting opinion in the case argued strenuously that school board officials, administrators, and teachers should be responsible for making decisions about the appropriateness of certain material for students, rather than the courts.⁶⁰

Filtering companies provide only limited information about their criteria for blocking and do not release lists of the sites that they have blocked. Some, but not all, filtering companies have close relationships with conservative religious organizations which appears to guide their filtering decision-making, but the companies do not disclose this bias in their advertising. It remains a major question of concern whether districts legally can *or should* turn over the responsibility of determining what their students can or cannot access to for-profit companies who do not fully disclose the basis upon which they are making their decisions.

D. Recommendations

- Distinguish two types of material that should not be accessed:
- Material that is prohibited—Profane or obscene (pornography), advocates or condones unlawful or

58. *Id.* at 569.

59. *Id.*

60. See Board of Educ. Island Trees Union Free Sch. Dist. No. 26 v. *Pico*, 457 U.S. 853 (1982).

dangerous acts, advocates or condones violence or discrimination towards other people (hate literature).

- Material that does not have an educational purpose.
- Provide staff monitoring of students, with back-up technical monitoring.
- Allow exceptions to prohibited material in cases of legitimate research.
- Teach students to self-monitor to determine appropriateness of material and activities.
- Establish a policy that students needing access for class projects have highest priority.
- Establish a process for students to notify staff if they mistakenly access prohibited material.
- Inform parents that the district cannot monitor in accord with a multitude of different family values. Encourage parents to discuss their values with children.
- If the school is having problems with inappropriate access the first issue to investigate is how prepared the teachers are to provide effective educational classwork using the Internet. The second issue to investigate is monitoring practices.
- If filtering software is used, exercise caution about the selection and configuration of the product.

VII. FREE SPEECH: ACADEMIC FREEDOM

Our nation is deeply committed to safeguarding aca-

democratic freedom, which is of transcendent value to all of us and not merely the teachers concerned, That freedom is therefore a special concern of the First Amendment, which does not tolerate laws that cast a pall of orthodoxy over the classroom. . . . The classroom is peculiarly the 'marketplace of ideas.' The Nation's future depends upon leaders trained through wide exposure to that robust exchange of ideas which discovers truth "out of a multitude of tongues, [rather] that through any kind of authoritative selection."⁶¹

The effort to pull ideology out of schools is evident in battles over history textbooks. . . . (M)ost students read carefully censored books. The pursuit of 'neutrality' often leads to censorship. The American Textbook Publishers Institute has counseled publishers 'to avoid statements that might prove offensive to economic, religious, racial or social groups or any civil, fraternal, patriotic, or philanthropic societies in the whole United States.' Textbook manufacturers appear to have responded in some cases by deleting materials reflecting cultural differences that might have offended someone. Interest group pressures from diverse ideological camps have resulted in the deletion of materials that would undercut the perception of an American monopoly on decency, as variously defined. Business interests have occasionally intervened in textbook selection to remove materials considered hostile to the "American system." American policy is sanitized. Books rarely report questionable government action.⁶²

Perhaps the most striking feature of history textbooks is that they minimize the role of dissent in our history. Government decisions that appear decent or beneficial are often portrayed without any of the political controversy that created them.⁶³

Most states and districts have established careful processes to determine what information is provided to students. This

61. *Keyishian v. Board of Regents*, 385 U.S. 589, 603 (1967) (citation omitted).

62. Susan Gottlieb, *In the Name of Patriotism: The Constitutionality of 'Bending' History in Public Secondary Schools*, 62 N.Y.U. L. REV. 497, 504 (1987) (citation omitted).

63. *Id.* at 505.

process also frequently acts in such a way as to limit exposure to controversial viewpoints or subjects. When teachers use the Internet with their students, decisions about the appropriateness of certain materials are no longer under the control of school textbook publishers or school textbook selection committees. The teacher bears the primary responsibility for the selection of materials. It is quite easy to anticipate that the use of the Internet in the classroom will provide a vehicle to expose students to a wide range of perspectives that have not traditionally been accessible in the classroom.

A. Guidelines for Teachers

Most districts have policies on academic freedom. It should not be necessary for districts to redo these policies to address the Internet access. However, it may be prudent for districts to provide recommendations to teachers on the material they select through the Internet for class reading.

- Teachers should select required or recommended material that is appropriate in light of the age of the students and that is the relevant to the course objectives.
- Teachers should, to the best of their ability, preview the materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site.
- Teachers should provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly when they are accessing the Internet independently. Lists of resources that are developed by educational groups are preferred.
- Teachers should assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

Clearly, the best way to avoid unnecessary controversy is to place a high priority on providing professional development opportunities for teachers to prepare them to handle this new learning environment. Districts that fail to provide for adequate teacher preparation will be the ones that face the greatest difficulties.

If we expect schools to be able to prepare students “for active participation in the pluralistic, often contentious society”⁶⁴ we could ask for no better source of materials to accomplish this than those found on the Internet. Although there may be some unsettling terrain to negotiate in the future, access to the Internet will indeed provide our students, our future citizens, with “wide exposure to that robust exchange of ideas” and, as a result, education will undergo profound change.⁶⁵

64. *Id.*

65. *Id.*