

THE LEGAL ASPECTS OF TECHNOLOGY IN THE SCHOOLS

Presented by Joanne Harmon Curry



740 Regent Street, Suite 400
Post Office Box 1507
Madison, Wisconsin 53701-1507
(608) 257-7766
info@lathropclark.com

I. Student Use and Misuse

A. School Discipline

1. *J.S. v Bethlehem Area Sch. Dist.*, No. 33 MAP 2001 (Pa. Sept. 25, 2002)

Issue: Whether a school district may discipline a student, consistent with the First Amendment, for creating a website at home and posting it on the Internet, when it contained derogatory, profane, offensive, and threatening statements directed toward a teacher and his principal who saw the site at school?

Facts: An eighth grade student created a website entitled “Teacher Sux” on his home computer, on his own time, and posted it on the Internet. The website was not sponsored by the school district. It consisted of web pages that made derogatory, profane, offensive, and threatening comments in the form of written words, pictures, animation, and sound clips. For example, it included a picture of his teacher with a severed head dripping with blood and a solicitation for funds to cover the cost of a hit man. One web page indicated that the principal engaged in sexual relations with a principal from another school. When the principal and teacher viewed the site at school, each took the threats seriously. The student was expelled from school and, subsequently, sued the school claiming First Amendment speech rights.

Holding: The Supreme Court of Pennsylvania affirmed the lower court ruling in favor of the school district. First, the court concluded that the student’s speech was not a “true threat,” an exception to the right of free speech, and cited the fact that the district allowed the student to attend class and extracurricular activities during an investigation of the incident. Second, however, the court concluded that although the website was created off-campus, it was accessed and viewed at school. In upholding the student’s expulsion the court reasoned that student free speech rights must be balanced with the school officials’ need to maintain order and to discipline when necessary to assure a safe school environment that is conducive to learning.

2. *Killion v. Franklin Reg’l Sch. Dist.*, 136 F. Supp. 2d 446 (W. D. Pa. 2001)

Issue: Whether a school district may discipline a student consistent with the First Amendment when he sends e-mails from home to friends’ homes that contain offensive and obscene language about the school’s athletic director?

Facts: A student created a “Top Ten” list about the school’s athletic director, including statements about the director’s physical appearance and genitalia, while at home after school hours. The student e-mailed the list from his home computer to friends at their homes. He did not print or copy the list to bring on school premises because he had been warned about such behavior after copying and distributing similar lists in the past. However, an unknown person brought the

student's list to campus and distributed it. The student admitted creating the list and was suspended for the offensive remarks about a school official in the list found on school grounds. The student sued the school claiming First Amendment speech rights.

Holding: The court ruled in favor of the student, finding the district violated the First Amendment because it failed to satisfy the "substantial disruption test." There was no evidence the teachers were incapable of teaching or controlling their classes because of the list, which was, in fact, on the campus for several days before the administration became aware of its existence, and the administration waited one week before taking any action. Furthermore, even though the list contained lewd and obscene language, which might be punishable in the school context, there was no evidence the student was responsible for bringing the list to school.

3. *Emmett v. Kent Sch. Dist. No. 415*, 92 F. Supp. 2d 1088 (W.D. Wash. 2000)

Issue: Whether the student's First Amendment rights were violated when the school district expelled him for intimidation, harassment, disruption to the educational process, and violation of school copyright rules because he posted a web page on the Internet from his home that consisted of mock obituaries?

Facts: Emmett created a web page from his home without using school resources or time that consisted of tongue-in-cheek, mock "obituaries" of two friends. A creative writing class in which students were assigned to write their own obituary inspired the page. Emmett also allowed visitors to the website to vote on who would "die" next, that is, who would be the subject of the next mock obituary. The website became a source of discussion at the school and on the evening news, it was characterized as featuring a "hit list" of people to be killed. The website, however, did not use the words "hit list" anywhere on the site. The school initially expelled Emmett, but modified it to a five-day short term suspension. The suspension included a prohibition on participation in school sports, including basketball practice and the team playoffs. The student sued the school seeking an injunction against the short-term suspension.

Holding: The court held for the student, finding that missing four additional days of school and sporting events would cause him irreparable injury when balanced against the hardships presented by the school district. The school district failed to show that any student actually felt threatened by the website, or that Emmett had any intent to intimidate or threaten anyone. Although the court sympathized with the school's concern that websites can be an early indication of a student's violent inclinations and can spread those beliefs quickly to like-minded or susceptible people, it rejected the school's claims that the suspension was necessary. The school's case was based on a lack of evidence, and the undifferentiated fear of possible disturbances or embarrassment to school officials was insufficient to support their claim.

6. State Legislation

Electronic Communication Devices Prohibited (Wis. Stat. § 118.258)

Each school board must adopt rules prohibiting students from using or possessing an electronic paging or 2-way communication device while on the premises of a public school and provide them to each student annually.

B. Criminal Conduct

1. *Boucher v. School Bd. of the Sch. Dist. of Greenfield*, 134 F.3d 821 (7th Cir. 1998)

Issue: Whether a student violated the state criminal computer law and school policies regarding student use of school district computers when he distributed an article at school entitled, “So You Want To Be A Hacker?”

Facts: Boucher wrote an article entitled “So You Want to be a Hacker” outside of school, published it in an underground, unofficial newspaper, and then brought it to school and distributed it in bathrooms, lockers, and in the cafeteria of Greenfield High School. The article described how to enter the computer’s setup utility, see a list of every file on the computer, with student and teacher login names, and attempt to find the password for entering the files. The Board concluded, that the article provided instruction to unauthorized persons on how to access the school district computer programs and disclosed restricted access information to the school district’s computers. Boucher was expelled for violating the Board policy on the use of the school district computers, network and the Internet and general school rules for behavior and communications by its students with its computers. Boucher sued the school district for violating his First Amendment right to speak freely on the subject of computer use and hacking.

Holding: The Seventh Circuit Court of Appeals found in favor of the school district, reversing the federal district court ruling. The court reasoned that “[t]he Supreme Court has repeatedly emphasized the need for affirming the comprehensive authority of . . . school officials, consistent with fundamental constitutional safeguards, to prescribe and control conduct in the schools.” The court found that the school district faced substantial harm when confronted by the self-proclaimed, student hacker if the district court injunction was enforced against their disciplinary efforts. The court concluded that the article, distributed on campus with the student’s knowledge, purported to be a blueprint for the invasion of the school’s computer system, as well as encouragement to do just that—a call to action detrimental to the tangible interests of the school and endangering school property.

2. *Spielmann v. Hayes*, 2000 Okla. Civ App 44, 3 P.3d 711

Issue: Whether the court could enforce a protective order obtained by a teacher against a student when the student left a voice mail threat on the teacher's school voice mail system directed at the teacher's husband?

Facts: A message was left on the 7th grade science teacher's school voice mail that threatened to kill her husband if she disciplined any students. When the teacher retrieved the message, she contacted the principal and two other administrators. The teacher recognized the voice as one of her students. The student was expelled from school. The teacher filed a petition for a protective order against the student as a victim of harassment, defined by the Oklahoma statutes under the Protection From Domestic Abuse Act. The trial court ordered the student not to abuse, injure, visit, threaten, or harass the teacher. The student challenged the order.

Holding: The court affirmed the order. Even though the threat was directed at the teacher's husband, the student had engaged in a course of conduct of choosing to leave a voice mail message containing an articulated death threat, alarming the teacher, causing her substantial emotional distress, and serving no other legitimate purpose than to require the teacher to alter her course of conduct by not sending any student to the office in order to avoid the death of her husband.

3. Federal Legislation

Child Online Protection Act (COPA) (47 U.S.C. § 231)

- a. This section of the law makes it a crime for commercial sites to knowingly distribute indecent material that is harmful to minors. Under the act, commercial web publishers are required to ensure that minors do not access the harmful material on their Website.
- b. Note: On May 13, 2002, the U.S. Supreme Court overturned a narrow lower court decision that COPA was unconstitutional because its definition of material harmful to minors included the application of "contemporary community standards." The Court explained that reliance on community standards was not enough to violate the First Amendment. The case, however, is proceeding again through the lower courts in a challenge to its constitutionality on other grounds.

4. State Legislation

a. Computer Crimes Act (Wis. Stat. § 943.70(2))

Willful, knowing, and unauthorized offenses against computer data and programs, including copying, modifying, destroying, accessing, or disclosing restricted access codes to unauthorized persons, of data, computer programs or supporting documentation is a crime.

b. Unlawful Use of Computerized Communication Systems (Wis. Stat. § 947.0125)

Intentional conduct consisting of frightening, intimidating, threatening, abusive, or harassing messages sent to a person on an electronic mail or other computerized communication system with the threat to inflict injury or physical harm to any person or property is a crime.

c. Harassment (Wis. Stat. § 947.013)

Harassment means a pattern of conduct or repeatedly committing acts representing a credible threat which harass or intimidate another person.

- (1) Harassment includes striking, shoving, kicking or otherwise subjecting another person to physical contact or attempting or threatening to do the same.
- (2) The statute refers to actions against a “person,” which has been interpreted by case law to include municipalities. A school district, therefore, is an entity entitled to obtain injunctions and may do so when there is a relationship between the harassing conduct and the school.
- (3) Case law confirms that the statute does not violate protected speech, rather, it is directed at oppressing repetitive behavior which invades another’s privacy interests in an intolerable manner.

C. Access to Internet Information: Filtering

1. *Mainstream Loudoun v. Board of Trustees of Loudoun County Library*, 24 F. Supp. 2d 552 (E.D. Va. 1998)

Issue: Whether a public library may enact a policy prohibiting the access of library patrons to certain content-based categories of Internet publications, violating the First Amendment?

Facts: The Loudoun County Library used filtering technology to limit patron access to some Internet sites, ostensibly as “an acquisition decision.” Adult patrons challenged the library’s use of X-Stop software to block Internet access to pornography on all library computers. The patrons claimed the practice was a violation of their First Amendment rights.

Holding: The court rejected the library’s position, holding that the act of filtering out certain Websites was a form of censorship and was not a process of selection, analogous to the purchasing of printed materials for the library. The court held that the library had created a limited public forum for both the expression and receipt of ideas. Another example of a limited or designated forum are school board meetings. Non-public forums were described as such forums as a government office building or a teacher’s mailbox. These types of forums are not by tradition or designation forums for public communication. Yet, once the government operates a limited forum, such as what the public library did, it must allow expressive activity. The government, however, can create this limited public forum for all, some, or only a single kind of expressive activity.

Here, however, the method used to filter information was over-inclusive and the technique lacked standards for selecting which sites would be blocked. The three factors that the court considers in distinguishing between a limited or non-public forum are government intent, extent of use, and nature of the forum. The court emphasize that its ruling applied only to public libraries, not public schools and involved the right of adults, not minor children.

2. Federal Legislation

a. Children’s Internet Protection Act (CIPA) (20 U.S.C. § 9134; 47 U.S.C. § 254)

As a general rule, school districts must enforce the installation and use of a “technology protection measure,” a specific technology that blocks or filters Internet access to prohibited Internet material. The technology protection measure must protect against Internet access for minors to visual depictions that are obscene or child pornography and from any picture, image, graphic image file, or other visual depiction that is considered harmful to minors.

- (1) Schools receiving universal service discounts (E rate money), Internet service, or internal connections or receive funds under the Library Services and Technology Act or Title III of the Elementary and Secondary Education Act to purchase computers for Internet access or pay for Internet services to comply with the Act.

- (2) An administrator, supervisor, or person authorized by the school district may disable the technology protection measure to enable access for bona fide research or other lawful purposes.
- (3) Schools must certify with the FCC that they are in compliance or risk losing funding, that is, that they have selected a technology and have implemented a policy to filter or block materials on computers with Internet access.

b. Communications Decency Act (CDA)—Protection for Private Blocking and Screening of Offensive Material (47 U.S.C. § 230)

- (1) This law provides, in part, that:
 - i) 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; and
 - ii) Disincentives are removed for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.
- (2) The law creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.

It provides for protection for “good samaritan” blocking and screening of offensive material. Providers or users of an interactive computer service will not be held liable on account of any action voluntarily taken in good faith to restrict access to or 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.

D. Privacy Rights: Personal Information

1. Federal Legislation

a. Children’s Online Privacy Protection Act (COPPA) (15 U.S.C. § 6501 *et seq.*)

- (1) COPPA regulates the collection, use, and disclosure of personal information from children under 13 years of age by Website and online service operators.
- (2) The law defines “operator” as any person who operates a Website located on the Internet or an online service, collects or maintains personal information from or about persons using or visiting the site, and operates the Website or service *for commercial purposes*, such as e-mail, a chat room or message board, which results in the public posting of personal information on a website or online service. It includes information that is collected using passive tracking or use of any identifying code linked to an individual, such as a “cookie.”
 - i) The law does not affect those operators who only provide access to the Internet for the sole purpose of obtaining information and with no interactive component.
 - ii) The operator of a site that only links users to a second site is not liable for violations occurring at the second site, although school districts may want to examine relationships with corporate affiliates, agents, and independent contractors to ensure compliance.

b. Personal Information Defined

Personal information means any identifiable information about an individual collected online, such as first and last name, home or other physical address, e-mail address, telephone number, and social security number.

c. If covered by the law, operators must:

- (1) Post a notice on the website of how personal information from children is collected, used, and disclosed. If a hyperlink is used on the homepage to allow users to obtain

the notice information, the link must be prominently displayed.

- (2) Notify parents if the operator wishes to collect information from their children and obtain verifiable parental consent before any personal information is collected, used, or disclosed.

Verifiable parental consent means making any reasonable effort to ensure that before personal information is collected from a child, a parent receives notice of the operator's information practices and consents to those practices. This can include allowing e-mail consent, but only if the parent and child have different e-mail addresses, or sending follow-up e-mails to the parent after initial notice attempts in order to increase the likelihood that the parent will see the request for consent.

- i) Never condition a child's participation in online activities on the provision of more personal information than is reasonably necessary to participate in the activity.
- ii) Allow parents the opportunity to review and have their children's information deleted from the database and to prohibit further collection from the child.

If the website or online operator combines information collected offline with information collected online, the operator must disclose all data in response to a parent's request for the information.

- iii) Establish procedures to protect the confidentiality, security, and integrity of personal information that you collect from children.
- (4) The federal rules regulating the law do not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parents' agent in the process. Where an operator, other than a school, is authorized by a school to collect personal information from children, after providing notice to the school of the operator's collection, use, and disclosure practices, the operator can presume that the

school's authorization is based on the school's having obtained the parent's consent.

**b. Family Educational Rights and Privacy Act (FERPA)
(20 U.S.C. § 1232)**

- (1) Because the storage media in which the school maintains student education records does not affect the student's privacy rights under FERPA, a student record may be a computer file or a computer printout. Parents or eligible students have the right to inspect and review all of the student's education records maintained by the school.

2. State Legislation - Right of Privacy (Wis. Stat. § 895.50)

- a. The right of privacy is recognized in this state.
- b. Exceptions: The U.S. Supreme Court has recognized that the uninhibited exercise of those rights may be hedged with restrictions that reflect the public policy of protecting persons of a distinct class. Therefore, the right of privacy as it relates to minors is dictated by state law.
- c. In Wisconsin the privacy rights of minors have been limited in several areas, suggesting some limitations on the minor's expectation of privacy, e.g., use of a minor for advertising purposes requires written consent of a minor's parent or guardian; parental consent is required prior to an abortion performed on a minor.

II. Employee Use and Misuse

A. Privacy Rights: Video Surveillance, E-mail and Voice Mail

1. *Vega-Rodriguez v. Puerto Rico Telephone Co.*, 110 F.3d 174 (1st Cir. 1997)

Issue: Whether the company's continuous video surveillance of the work area violated privacy rights and Constitutional protections?

Facts: Puerto Rico Telephone Company is a quasi-public corporation. Employees sued the company challenging videotaping of their workplace as an invasion of their privacy and a violation of the Fourth Amendment Rights. The work space inside the company's Executive Communications Center consists of a large L-shaped area containing computers, monitors, furniture, etc. The work space is completely open and no individual employee has an assigned office,

cubicle, work station, or desk. Three video cameras survey the work space, and a fourth tracks all traffic passing through the main entrance. Cameras do not cover the employee rest area. The surveillance is exclusively visual; the cameras have no microphones or other immediate eavesdropping capability and operate all day, every day. No one is allowed to view the monitor or completed tapes without the general manager's express permission.

Holding: The court upheld the use of video surveillance of employee work space. First, the court reasoned that business premises invite lesser privacy expectations than do residences. Second, the court found that the physical layout of the work area belied any expectation of privacy. Third, the court found that the nature of the intrusion, monitoring space that is in plain view within an open area, strengthened the employer's legitimate interests. Finally, the court noted that employer policies and regulations can provide a warning to employees that certain areas are subject to employer intrusions, reducing their expectations of privacy. The court concluded that unconcealed video cameras not equipped with microphones, which record only what the human eye could observe, did not violate the employee's privacy or constitutional rights.

2. *Cramer v. Consolidated Freightways Corp.*, 209 F.3d 1122 (9th Cir. 2000), cert. denied, 122 S.Ct. 806 (2002).

Issue: Whether privacy rights were violated when the company surreptitiously videotaped restrooms through two-way mirrors when the collective bargaining agreement with the union included the use of video cameras?

Facts: Several truck drivers brought a class action suit against a California trucking terminal alleging invasion of privacy and infliction of emotional distress when it was discovered that the company was videotaping in the restrooms. California law prohibits placing cameras or two-way mirrors in restrooms. The case became known as the "potty privacy" controversy. The company said it installed the cameras to try to stop the sale and use of drugs in the restrooms and aimed the cameras away from urinals and toilets. It claimed that the Union had agreed to video surveillance as part of an employment contract and, therefore, could not expect privacy even in the lavatory.

Holding: The court dismissed the invasion of privacy and infliction of emotional distress claims because the collective bargaining agreement allowed both video surveillance and drug testing. The court agreed with the trucking company that the privacy claim could not be determined without interpretation and application of the collective bargaining agreement because the employees alleged that they reasonably expected to be free from video surveillance. The claims, therefore, fell within the preemptive reach of the Labor Management Relations Act, 29 U.S.C. § 185. One judge dissented, however, quoting from George Orwell's classic novel, *1984*. He raised the concern that Consolidated's restroom

surveillance was a clear violation of California law and that collective bargaining agreements cannot contract for illegal activities.

3. *Thompson v. Johnson County Community College, No. 96-3223, 1997 U.S. App. LEXIS 5832 (10th Cir. March 25, 1997) (unpublished)*

Issue: Whether silent video surveillance of an employee locker area violated employee privacy rights?

Facts: Security officers at a community college had a locker area in a room that also housed the heating and air conditioning equipment for the college and which served as a storage area. Individuals other than the security officers could freely enter the room at any time. The room was not locked and access was not restricted to those with legitimate business in the room. The room was equipped with a silent video surveillance camera. The security officers alleged that the video surveillance violated the Electronic Communications Privacy Act (ECPA) and their Fourth Amendment privacy rights.

Holding: The court held that silent video surveillance, i.e., video surveillance without audio capability, is not covered by the ECPA. Therefore, silent video surveillance did not violate the Act. Employees may be able to assert a right to privacy in their personal locker space, and other areas such as a locked desk, when adequate notice is not provided that such areas may be subject to unconsented searches. However, they do not have a reasonable expectation of privacy in the area surrounding a locker and other public or semi-public space. The fact that few people other than the security officers entered the room did not change the court's analysis.

4. *Service Employees International Union, Local No. 152, AFL-CIO Racine Unified Sch. Dist., Case 191, No. 58280, MP-852.3.2, Dec. No. 29846-B (WERC, 2/2001)*

Issue: Whether the School District's decision to install and utilize hidden video cameras on the loading dock and in the break room for the purpose of theft detection was a permissive subject of bargaining?

Facts: The School District installed and used hidden video cameras on the loading dock and in the break room because of concerns with the need for theft detection. Neither camera recorded sound. The School District installed the hidden video cameras after complaints from a number of employees at an elementary school indicated that the building service employees were taking extended lunches and breaks, standing around a lot, and taking school lunches for free. The video cameras were installed at the loading dock and in the break room to investigate these allegations.

The Union found out about the video cameras and filed a complaint with the Wisconsin Employment Relations Commission (WERC), claiming the practice was primarily related to wages, hours, and terms and conditions of employment, specifically, job security. The Union also raised privacy concerns. The District claimed the hidden video cameras were a legitimate investigatory or information gathering tool used to safeguard District property or the health, safety and welfare of its employees and students. The Union did not request that the District bargain over either its decision to install and utilize hidden video cameras, or the impact of the District's decision.

The WERC Examiner found for the District. The Union then appealed to the Commission.

Holding: The Wisconsin Employment Relations Commission affirmed the WERC Examiner's finding that under the facts of this case the use of hidden video cameras was not a mandatory subject of bargaining within the meaning of Wis. Stat. § 111.70(3)4 or derivatively 1. The School District's decision to install and utilize hidden video cameras on the loading dock and in a break room to investigate allegations of employee misconduct primarily relates to the management and direction of the School District and the formulation or management of public policy.

The Commission distinguished the instant case from the employees/unions right to bargain for a disciplinary process which will give them notice of the employer's expectations for their job performance, notice when they are failing to meet those expectations, and opportunities to correct any performance deficiencies. Here, the misconduct in question was theft of property or time, and there are no issues of notice or knowledge of expectations. The Commission noted that the employees know they are not allowed to steal property or time.

5. *Bohach v. The City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996)

Issue: Whether the government department's retrieval of messages stored on the computer network violated federal wiretapping statutes and the employee's constitutional right to privacy?

Facts: The city police department used a software program that allowed the transmission of brief messages to visual display pagers. These are considered electronic communications that fall within federal law. An order issued by the chief of the department warned all users that every message was logged on the network, and that some types of messages were prohibited. The officers involved in the case sent messages to one another that were subsequently used during an internal affairs investigation against them. The officers claimed a violation of the Fourth Amendment prohibition against unreasonable searches.

Holding: The court found that the officers did not have an objectively reasonable expectation of privacy in the messages. To prevail on their claim, the officers had to demonstrate that they had a reasonable expectation of privacy in their use of the message system. The court distinguished between the transmission or transfer phase of the communication and the electronic storage of the messages. The court reasoned that the city was the “provider” of the “electronic communications service,” including the computer terminals, computer and software, and the pagers issued to personnel. These items provide the user the ability to send or receive electronic communications. The law allows providers of these systems to access stored electronic communications.

2. Federal and State Legislation

a. Electronic Communications Privacy Act (ECPA) (Federal Wiretap Act) (18 U.S.C. § 2510-2521; Wis. Stat. § 968.31)

- (1) It is unlawful to *intercept* and disclose wire, oral, or electronic communication, including telephone conversations and e-mail, while it is in transit.
- (2) An electronic communication consists of the *transfer* of the signals, data, and other items, but does not include their electronic storage. Interception occurs when it is captured or re-directed in any way through the use of a mechanical or electronic device. This may include obtaining access to in-storage wire communications (e.g., obtaining access to someone’s voice-mail mailbox and forwarding it to your own).
- (3) Ordinary course of business exception: the employer is allowed to monitor or record employee communications if it is done for a legitimate purpose and all employees have been informed about the monitoring device. It may be limited, however, to determining whether the nature of the communication is business related. The employee must be given prior notice.
- (4) Consent exception: It is not unlawful to intercept communications, such as e-mail and voice mail, while it is in transit if one party to the communication has given his or her consent to the interception. This may be inferred either through an employment contract or through a well disseminated e-mail policy.

**b. Electronic Communications Privacy Act (ECPA)
(Stored Communications Act) (18 U.S.C. § 2701-2711)**

- (1) It is unlawful to access *stored* electronic communications, such as e-mail, pagers, and voice mail, while it is in electronic storage.
- (2) Whoever intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility, and thereby obtains, alters, or prevents authorized access to an electronic communication while it is in electronic storage in such system shall be punished. Accessing e-mail from a stored database without authorization is prohibited, including read or sent e-mail that is saved on the user's server or hard drive.
- (3) Provider exception: the prohibitions against accessing stored electronic communications do not apply to conduct authorized by the person or entity providing an electronic communications service. The provider is the entity that provides the terminals, computers, software, pagers, etc. Therefore, if an employee provides access to e-mail through an in house e-mail server, the employer is free to monitor an employee's stored e-mail. This may not apply if access to e-mail is provided through a commercial Internet service provided, such as America Online.
- (4) User exception: the prohibition does not apply to users of the service with respect to a communication of or intended for that user. This exception includes individuals who expressly or impliedly have been given authorization to access the user's stored e-mail.
- (5) Ordinary course of business exception: a person or entity may divulge the contents of a communication as authorized under § 2511(2)(a) (see previous section).
- (6) Although the law is unclear regarding employer rights in this area, it is best to provide employees with prior notice of the employer's intent to monitor employee stored e-mail.

B. Privacy Rights: Employer Searches

United States v. Simons, 206 F.3d 392 (4th Cir. 2000)

Issue: Whether a government employer conducted an unlawful search of materials received by an employee at his government workplace via the Internet when it suspected a violation of workplace rules?

Facts: The government agency instituted a policy regarding Internet usage by employees. It stated that employees were to use the Internet for official government business only. Accessing unlawful material was specifically prohibited. The policy also explained that the agency would conduct electronic audits to ensure compliance that consisted of periodic auditing, inspecting, and/or monitoring the user's Internet access as deemed appropriate (which included e-mail messages).

While examining the agency's firewall log, the system administrator discovered evidence that the employee was accessing child pornography sites while at work. The systems administrator had noticed that the log was unusually large, and searched the log using the keyword "sex." Because the search generated a large number of "hits" traceable to the employee's workstation, indicating intentional Internet searches (rather than casual or accidental), the supervisor had the systems administrator access the employee's workstation computer to see if the employee had downloaded any pornographic pictures or files. Over one thousand pornographic files had been downloaded. A criminal investigation was initiated and a search warrant was obtained for the employee's office, including the computer and contents of its drive. The employee was indicted on one count of knowingly receiving child pornography in violation of a federal criminal law. The employee moved to suppress the evidence because of an illegal search in violation of his Fourth Amendment rights.

Holding: The court held that the agency's policy limiting the Internet to official purposes and giving notice that audits may be done on unclassified networks was sufficient to eliminate any reasonable expectation of privacy the employee had regarding his Internet use. Additionally, the systems administrator had a duty to monitor Internet use, including inappropriate workplace activity, as part of his official duties. The searches, therefore, were not illegal.

C. Government Regulation and Civil Prohibition of Employee Computer Usage

1. *Urofsky v. Gilmore*, 216 F.3d 401 (4th Cir.), cert. denied, 531 U.S. 1070 (2001)

Issue: Whether a state regulation prohibiting state employees' access to sexually explicit material on state computers is consistent with the First Amendment and their right to academic freedom?

Facts: Six professors employed by various public colleges and universities brought suit against the state of Virginia, challenging a law restricting state employees from accessing sexually explicit material on computers that are owned or leased by the state without permission.

Holding: The court held that regulation of state employees' access to sexually explicit material, in their capacity as employees, on state computers is consistent with the First Amendment. The court cited judicial precedence for the proposition that the state, as an employer, possesses greater authority to restrict the speech of its employees than it has as a sovereign to restrict the speech of ordinary citizens. The threshold question is whether the state law regulates the speech of state employees on matters of public concern in their capacity as citizens. Additionally, the court found no judicial support for a right to academic freedom above the protections afforded to all public employees against dismissal for the exercise of First Amendment rights.

3. *Strauss v. Microsoft Corp.*, 814 F. Supp. 1186 (S.D.N.Y 1993)

Issue: Whether e-mail messages could be used to support a claim of sexual harassment and discrimination?

Facts: A female employee at Microsoft received at least four separate e-mail messages from a supervisor that "contained sexual innuendo," such as referring to another woman in the office as the "Spandex Queen." She sued Microsoft for gender discrimination, relying, in part, on the e-mail messages as evidence. The supervisor had put the e-mail messages into personal folders on his work computer with his own password. The company policy allowed employees to do that, and the supervisor thought the messages were, therefore, secure. However, during the investigation of the supervisor, the company "broke into" the personal files and retrieved the messages. The defendant challenged the use of the e-mail messages as evidence at the trial.

Holding: The court ruled that the e-mail messages were admissible as evidence at the trial.

4. ***Greenslade v. Chicago Sun-Times, Inc.*, 112 F.3d 853 (7th Cir. 1997)**

Issue: Whether the frequency with which an employee sent unwanted e-mail messages to a coworker contributed to a finding of harassment?

Facts: Editors at the newspaper frequently communicated with coworkers about both business and personal matters via an electronic mail (e-mail) system. Greenslade was an editor who had created an inventory of multi-colored “form” e-mail messages for business and personal reasons which could be sent quickly to one or more coworkers. Included among his “form e-mails” was one in which he offered rides home to coworkers who had not driven to work. Shortly after a female coworker, Wagner, began work at the paper, Greenslade began offering her rides home. She initially accepted some of these offers. However, over a period of time, the quantity and content of e-mail messages Greenslade sent Wagner began to concern her. She was receiving more personal e-mails from Greenslade than from anyone else at the newspaper. Greenslade was removed from his position and transferred to another position with the company. He challenged the transfer.

Holding: The court ruled in favor of the company, finding that Greenslade engaged in unwanted, questionable behavior, in part, because of the *excessive number* of personalized e-mails he had sent Wagner.

5. ***Blakey v. Continental Airlines, Inc.*, 164 N.J. 38 (N.J. 2000)**

Issue: Whether an employer, who has notice that co-employees are engaging in retaliatory harassment directed at another co-employee by using a computer bulletin board created by the company, has a duty to remedy that harassment?

Facts: A female pilot filed systematic complaints with representatives of Continental Airlines, complaining of sexual harassment and hostile work environment based on conduct directed at her by male co-employees in the plane’s cockpit and other work areas. The conduct included displays of pornographic photographs and vulgar gender-based comments. When Continental failed to remedy the hostile work environment, the pilot filed a charge of sexual discrimination and retaliation in violation of Title VII of the Civil Rights Act.

In the midst of the federal litigation, fellow pilots continued to publish a series of harassing gender-based messages on the pilots’ on-line computer bulletin board. The bulletin board was accessed through the company’s Internet provider, where a forum for Continental pilots and crew members was available. Individual postings stated that the female pilot’s allegations were false, that the lawsuit was

motivated by greed and selfishness, that she had poor piloting and interpersonal skills, and that female pilots were looking for favorable treatment. One example was a posting stating, “I also heard you crashed your floatplane . . .,” which the female pilot called false and defamatory.

Holding: The state supreme court held that the electronic bulletin board should be regarded as part of the workplace, and that the postings could have constituted a hostile work environment. Furthermore, “when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace and in settings that are related to the workplace,” employers have a duty to take effective measures to stop co-employee harassment.

D. Criminal Conduct

1. *United States of America v. Hibbler*, 159 F.3d 233 (6th Cir. 1998)

Issue: Whether the defendant principal found guilty of possessing and distributing child pornography through his home computer should receive an enhanced criminal sentence even though the distribution did not include monetary sales or pecuniary gain?

Facts: A high school principal purchased a home computer and opened an account with America Online to obtain access to the Internet. He created the screen name “SHIGUY5811” and a false profile, claiming to be a student born in 1976 whose hobbies included trading “gifs” (i.e., on-line pictures) depicting child pornography. Through an FBI investigation, a search warrant was executed at the principal’s home, and over twenty-one images of child pornography were found on the computer hard-drive. The principal claimed he was “investigating” the accessibility of pornography on the Internet because his school was in the process of going on-line.

However, the school district did not have any plans to connect to the Internet or to provide on-line services. Furthermore, the principal was not a member of, or a consultant to, the committee responsible for developing and carrying out the network upgrading plan. The principle was charged with a seventeen-count indictment of conspiracy to ship and receive images depicting child pornography, receiving by computer transmission sexually explicit images of children, sending such images by computer, and possession of at least three computer files containing visual images of child pornography, in violation of 18 U.S.C. §§ 371, 2252(a)(2), 2252(a)(1), and 2252(a)(4). The district court identified “society” as the victim and combined the criminal counts into one offense for sentencing.

Holding: The court of appeals ruled that the sentencing court must impose an enhancement to the sentence because the conduct consisted of multiple offenses. It found that children depicted in child pornography are the “primary victims” of the crimes, even if they cannot be identified. In addition, the court of appeals held that distributions and transactions for pecuniary gain under the statutes include swaps, barter, in-kind transactions and other valuable considerations, not just monetary transactions. The cause was remanded for resentencing.

2. Federal Legislation

a. Protection of Children Against Sexual Exploitation (18 U.S.C. § 2252)

A crime is committed when any person knowingly transports or receives in interstate commerce, including by computer or mail, any visual depiction, if (a) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (b) such visual depiction is of such conduct.

3. State Legislation

a. Possession of child pornography (Wis. Stat. § 948.12)

Whoever knowingly possesses any undeveloped film, photographic negative, photograph . . . pictorial reproduction or audio recording of a child engaged in sexually explicit conduct is guilty of a felony.

III. Administrative Issues

A. Union Issues

1. *Timekeeping Systems, Inc. and Lawrence Leinweber, 323 N.L.R.B. 244 (1997)*

Issue: Whether the employee's sending of e-mail to fellow employees regarding the company's proposed change in the vacation policy was a "concerted activity" under the National Labor Relations Act?

Facts: Leinweber was a software engineer who worked for a 23-employee, family-owned business in Cleveland, Ohio. The company CEO sent out an e-mail to all employees regarding a proposed vacation policy change and stated that it would result in more days off each year for the employees. Leinweber did some calculations and discovered that the proposed policy would not, in fact, result in increased time off. He informed the CEO of his calculations and received no reply.

A member of the engineering team responded to the CEO's proposal with one word, "GREAT!" and sent the e-mail to all employees. Leinweber returned the e-mail informing the member of his calculations, then sent a lengthy e-mail message to all employees with similar information. The message called the CEO's description of the vacation policy "false."

The CEO was upset, told Leinweber he should have handled the criticism privately, and asked Leinweber to write an explanation of why this was not proper and how it hurt the firm. Leinweber declined to respond and was terminated from the company. Leinweber brought charges against the company alleging discharge for "protected concerted activity" under the National Labor Relations Act.

Holding: The National Labor Relations Board found that Leinweber's activity was "protected concerted activity" for the "purpose of mutual aid or protection," and that he was unlawfully fired. Leinweber was communicating with his fellow employees, attempting to correct any misimpression they had of the vacation proposal.

2. *E.I. DuPont DeNemours & Co., 311 NLRB 893 (1993)*

Summary: DuPont had a policy allowing for the use of the company e-mail system for personal use, but not for the solicitation or distribution of union materials. The policy resulted in differential treatment because committees could send notices over the e-mail system and employees were allowed to send messages on a variety of non-work topics. The National Labor Relations Board ruled that this policy violated employee rights by discriminating against the union.

3. *National Tech Team, Inc., No. 16-CA-20176, 2000 N.L.R.B. GMC LEXIS 30 (2000)*

Summary: Pratt & Whitney had a policy prohibiting personal use of the company e-mail system. When an employee sent union related e-mail messages to fellow employees, he was suspended from his job. The employees filed a complaint with the National Labor Relations Board on whether a company may issue a complete ban on all nonbusiness use of e-mail, which necessarily includes “employees’ messages otherwise protected” by federal labor law. The general counsel issued a memorandum concluding that the company e-mail policy was unlawful because it was overly broad and illegal on its face, restricting solicitation even during nonwork time.

4. *University of Wisconsin Hosp. And Clinics Auth., WERC Dec. No. 30202-B (Nielsen, 2002).*

Summary: The union representing the nurses employed by the University of Wisconsin Hospital and Clinics Authority regularly used the Hospital’s computer system to communicate with its members. Without warning, the Hospital began blocking the non-employee union representative’s e-mail messages. The union filed a prohibited practice complaint alleging that the Hospital’s actions interfered with the employees’ rights under the Wisconsin Employment Peace Act (WEPA). The Hearing Examiner concluded that sending union-related e-mail messages may constitute protected, concerted activity under WEPA. The Hearing Examiner held that employers must have a valid business reason to prohibit communication between employees regarding union-related issues and employers may not single out and prohibit employees from sending union-related e-mail messages. Presently, the full Commission is reviewing Nielsen’s conclusions to determine the law in Wisconsin on this issue.

5. *Organized Labor Activities and Employee Use of E-mail*

- a. An outright ban on employee use of e-mail for the disbursement of information associated with collective bargaining issues may be in violation of the National Labor Relations Act.
- b. The National Labor Relations Board (NLRB) has yet to decide whether e-mail usage is more akin to a posting on a bulletin board or to use of a company telephone.
- c. Unions are increasingly bringing the right to unmonitored Internet access and e-mail usage for employees to the bargaining table. The Wisconsin Employment Relations Commission (WERC) has not issued a ruling on whether such subjects are mandatory or permissive subjects of bargaining.

B. E-mail in Litigation

1. *Ellison v. Premier Salons Int'l*, 981 F. Supp. 1219 (D. Minn. 1997)

Summary: An employee relied in part on e-mail from a supervisor to make an age discrimination claim following his termination. The supervisor had sent an e-mail message stating, among other things, that it was “great to see someone of your age accomplish something like this!!! You and George Burns are an inspiration to the elderly EVERYWHERE!!!” Although the court rejected the employee’s claim, finding that it did not reflect a discriminatory attitude, the employer was forced to incur the cost and embarrassment of defending the e-mail in court.

2. *Spelios v. Aetna Life Ins. Co.*, 1999 U.S. Dist. LEXIS 10254 (D. Conn. 1999)

Summary: A discharged employee claimed age discrimination in part on an e-mail message sent by a younger supervisor who reported to him, and who replaced him upon his termination. “Subject: Happy 50. Left you a voice mail letting you know that I didn't forget you really are officially old . . . I hear the AARP literature is really good . . . So when are you going to retire so I can take your place ?” The court reasoned that the ADEA does not make all discussion of age taboo, and that there must be a nexus between the alleged age-related comments and the plaintiff’s termination. The Court declined plaintiff’s invitation to consider an obviously light-hearted joke from a subordinate as an inference of age discrimination.

3. Defamation

Employers may be libel for the e-mail or Internet-related activities of their employees, although the issue has yet to be decided by the courts. In many cases, employee e-mail or postings may carry the school district’s name. Therefore, defamatory statements sent by employees could be attributed to the district. As such, it is important for employees to be aware that the same discretion that they are expected to use in any written communication also applies to communication via the Internet.

C. Public Records

1. State Legislation

a. Definitions (Wis. Stat. § 19.32(2))

“Record” means any material on which written, drawn, printed, spoken, visual or electromagnetic information is recorded or preserved, regardless of physical form or characteristics, which has been created or is being kept by an authority. “Record” includes, but is not limited to, handwritten, typed or printed pages, maps, charts, photographs, films, recordings, tapes (including computer tapes), computer printouts and optical disks.

“Record does not include drafts, notes, preliminary computations, and like materials prepared for the originator’s personal use or prepared by the originator in the name of a person for whom the originator is working; materials that are purely the personal property of the custodian and have no relation to his or her office.”

b. Limitation Upon Access and Withholding (Wis. Stat. § 19.36(4))

Material used as input for a computer program or the material produced as a product of the computer program is subject to the right of examination and copying.

2. *State ex rel. Milwaukee Police Ass’n v. Jones*, No. 98-362998-3629 (Wis. Ct. App. 2000)

Issue: Whether the original digital audio tape recording from a telephone call is subject to the open records law?

Summary: The Milwaukee Police Association (MPA) requested a copy of a 911 telephone call from the City of Milwaukee Police Department (Department) under the open records law. The Department provided MPA with an analog tape recording of the call. MPA responded by specifically requesting access to the original 911 tape for the purpose of non-destructive analysis and/or making a digital audio tape (DAT). The Department denied the request to access the original recording. MPA petitioned for writ of mandamus, claiming that the Department violated the open records law.

The court of appeals affirmed the lower court’s holding that the Department was required to produce the original DAT recording for MPA’s examination and copying. In interpreting the open records statute, Wis. Stat. § 19.36(4), the court concluded that MPA must be given access to the source “material” and the opportunity for “examination and copying.” In declining to accept the

Department's argument, the court reiterated that "[t]here is a presumption that the public has the right to inspect public records unless an exception is found." The court noted the need to adhere to the spirit as well as the letter of the open records law.

3. *Wisconsin School News, Records Retentions Schedules (October 2002)*

Issue: Whether electronic material received by school board members at their homes is a public record under state law?

Summary: School board members who create or receive electronic district-related material at their homes that may be records of the school board should consider routing such items to their district for proper retention, including e-mail received on a personal account. The Public Records Law pertains to all forms of records, including e-mail and other forms of records that may exist in the future. A requestor of a public record may have a right to access to an electronic record in its original format where the custodian retains the record in its original format and there is some demonstrable need. *See State ex. rel. Milwaukee Police Assn. v. Jones*, 2000 WI App 146, 237 Wis. 2d 840, 615 N.W.2d 190.

E-mail correspondence and the equipment that stores them may also be accessed under the auspices of litigation and discovery requests.

D. Open Meetings

1. *Opinion to Paul E. Kritzer, Wisconsin Attorney General (August 20, 1996)*

Issue: Whether e-mail communications between the University of Wisconsin - Madison Athletic Board members, resulting in a decision to enter into a contract with Reebok International, Ltd., was a violation of the open meetings law?

Summary: The Attorney General concluded that the e-mail communications between Athletic Board members probably constituted a "meeting" in violation of the open meetings law. The chairman of the board had indicated that he would need to poll a sufficient number of board members in order to finalize a decision regarding Reebok's contract. The Attorney General based his opinion, in part, on a court decision in which the definition of "meeting" was determined to include "walking quorums," i.e., a series of gatherings among separate groups of members, each less than quorum size, who agree, tacitly or explicitly, to act uniformly in sufficient number to reach a quorum.

2. *Del Papa v. Board of Regents, 956 P.2d 770 (Nev. 1998)*

Issue: Whether board members' communications by facsimile and voice mail regarding a board issue violated the Open Meeting law?

Summary: One Board member made public comments critical of certain Board procedures. The Board Chairman prepared and disseminated a facsimile transmission to all members of the Board except the complaining Board member. The communications was a media advisory in response to the public complaints. Board members were to respond by telephone calls or messages. The Attorney General filed a lawsuit charging the Board with violating the Open Meeting law.

Open meeting laws are governed by state statute. The Nevada statute specifically says, “electronic communications must not be used to circumvent the spirit or letter” of the law “in order to discuss or act upon a matter over which the public body has supervision, control, jurisdiction or advisory powers.” However, the court also considered several other issues, including the definition and interpretation of a “meeting” and the term “present.” The court concluded that because there was a quorum, government resources were used, and the conduct was related to developing Board policy, including taking action on the material by deliberating toward a decision, that the Board had acted in its official capacity as a public body.

IV. Acceptable Use Policies (AUPs)

A. Employee AUPs: Developing an Acceptable Use Policy

1. Written Agreements

Acceptable Use Policies, or “AUPs,” often take the form of written agreements between employers and employees, and, at a minimum, set forth permissible uses of the Internet and e-mail.

2. Reasons for implementing an AUP

- a. To address/prevent lost productivity.
- b. To provide a shield against liability.
- c. To address technological and budgetary concerns.
- b. To provide uniformity and fairness. All employees’ expectations of privacy are equitably limited by AUP’s. Also, discipline for inappropriate use can be more readily justified and evenly applied.

B. Non-Exhaustive Checklist of Elements for an AUP

1. Purpose

A purpose statement will often provide that the agreement is intended to identify the appropriate use of e-mail and the Internet, establish ownership of information, define limits of personal privacy, and state specific prohibitions. It should include a statement that the computers and their software are educational tools owned by the district.

2. Privacy of Communications

It is important to state clearly that Internet and e-mail communications are not private. An employer may also warn employees that e-mail is significantly less secure than other traditional forms of communications because messages can be printed and backed-up on disk.

3. Monitoring

If the employer wants to monitor such activities, it is advisable to include a statement in an AUP that the employer reserves the right to monitor and access an employee’s Internet activities and e-mail account at all times and without notice.

4. Access and Identification of Authorized Users

It is worthwhile to identify authorized users, define access limitations, require use of passwords and ensure that employees shut down their terminals at the end of each day to help control access.

5. Unacceptable Use Computer Systems

When drafting an AUP, employers must determine what activities to prohibit, e.g., use for personal business, soliciting or lobbying for political or religious causes, use for unethical or disruptive activities, sending junk mail or chain letters for becoming a member of non-work related listserves.

6. Nondiscrimination and Sexual Harassment

An AUP should contain a statement which is consistent with the employer's general policy on sexual harassment and discrimination. For example, a statement may provide that neither e-mail nor the Internet should be used to send jokes or other comments that may be discriminatory, harassing or offensive to others or material that defames an individual, company or business, or discloses personal information without authorization. Penalties may include criminal sanctions under Wis. Stat. § 947.0125 for threatening, abusive, or intimidating messages sent to another person through e-mail or other computerized communication system. Employers should also advise that, while monitoring may occur, it is not possible to check and evaluate every communication and, therefore, employee reporting is essential to address harassment.

Provide notification, consistent with the employer's policy on sexual harassment, that employees are not to access pornographic sites or display images of a sexual nature on their monitors. Penalties for such use may include criminal sanctions under 18 U.S.C. § 2252 and Wis. Stat. §§ 948.11, 948.12.

7. Restrictions on Copying and Distribution of Electronic Messages

An AUP may define the duration and method of retention for all of the employer's electronic records. It may include a statement of copyright restrictions, including the illegal copying or publication of material in digital format. Penalties may include personal liability when employees violate copyright laws.

8. Supervisory Responsibility and Enforcement

An AUP may identify personnel who are responsible for enforcement and administration of the AUP. An enforcement section may describe procedures for identifying and investigating incidents of unauthorized system use. This section might include:

- a. Identification of the person(s) in the organization that is to be notified upon discovery of an incident that violates the provisions of an AUP.
- b. Instructions regarding how the person to be notified of such incidents should be apprised of the situation.
- c. Instructions advising individuals who discover evidence of unauthorized use to immediately print and preserve a hard-copy version of monitor screens that substantiate the incident.

9. Penalties

An AUP should contain a statement regarding the penalties for violating the agreement including, but not limited to, termination, revocation, suspension, and potential criminal sanctions. The AUP may include a statement that user access may be terminated if identified as repeat offender.

10. Consent Form

A consent form should accompany the policy, whereby an employee acknowledges and agrees to the provisions of the AUP. The form should state that the employee is consenting to the monitoring and access of both their e-mail and Internet usage.

11. Copy of Agreement

A copy of the AUP should be given to all employees in hard copy, and, generally, a signed acknowledgement should be secured from the employee. Copies of the AUP should be delivered in hard copy form and not only by electronic methods. One New Jersey court found that distribution by e-mail was an ineffective method of distributing a company policy. See *In re Prudential Ins. Co. Sales Practices Litigation*, 169 FRD 598 (D. N.J. 1997).

C. Student AUPs

1. In addition to the provisions contained in the employee AUP, a student AUP should also include the following elements:
 - a. A statement that Internet usage is a privilege, not a right.
 - b. A statement regarding a pupil's potential exposure to obscene or objectionable material.
 - c. A statement regarding the penalties for failure to abide by the policy.
 - d. Parental authorization for a pupil's use of the Internet, including a statement and signature reflecting the consent to the monitoring and interception of the pupil's Internet and e-mail activities.
 - e. Parental notification and verifiable consent if the school operates a website or online service and collects or maintains personal information from or about children under the age of 13.

2. The statement on penalties for failure to abide by the policy should be, to the extent possible, consistent with existing policies for misbehavior and the use of print media. Possible penalties include:
 - a. Revocation of Internet or e-mail privileges.
 - b. Student discipline including suspension or expulsion depending on the behavior in question.
 - c. Criminal sanctions under Wis. Stat. § 947.0125 for threatening, abusive, or intimidating messages sent to another person through e-mail or other computerized communication system.
 - d. Criminal sanctions under Wis. Stat. § 943.70 for offenses against computer data and programs, including copying, modifying, accessing, destroying, or disclosing restricted access codes to unauthorized persons, of data, computer programs, or supporting documentation.

D. Community AUPs

When a school district opens the access and use of its electronic communications and information processing equipment to its community members, it should consider developing policies with some of the following elements:

1. A clear statement that the district's Internet and online services are for the specific and limited purpose of enhancing the delivery of educational material, consistent with the educational mission of the school. As such, it should be understood as a limited purpose network and distinguished from a general personal account. Community members should be made aware of the fact that use of the school's service may be provided with restrictions consistent with the school's educational mission and goals.
2. A statement that users should have no reasonable expectation of privacy and that the district reserves the right to monitor and access Internet activities and e-mail content; consider a statement reminding them that they may avoid exposing personal material by simply not using the district's Internet and on-line facilities to communicate or to record such information.
3. A statement describing the district's regulation of access to Internet content (e.g., filtering software) and e-mail services in light of its compelling governmental interest in protecting minors from harmful material. By providing community access, the school may be creating a public forum. This would be analogous to providing public use and access to the school's physical property.

Alternatively, the district could consider regulation of community members' use and access to the district's services based on time, place, and manner. Alternatives to content-based restrictions include the acceptable use policy, educating patrons, time limits on usage, turning filters off for adult use or using filters on only some machines, relocating terminals, enforcing criminal laws, and using privacy screens.

4. A clear rule for revoking a community member's use of the district Internet and e-mail services. The district has the right to discontinue the use of any property not required for school purposes. The standards for revoking the user privilege should have sufficient specificity to withstand charges of vagueness or overbreadth, i.e., too sweeping in coverage. Procedural safeguards should be considered.
5. A disclaimer of warranties, that is, of any responsibility for the accuracy or quality of information, responsibility for any loss of data, or unavailability of the system, and a statement that reliance on the system is at the user's own risk. Consider requiring that users agree to indemnify

the school district for any expense incurred from violation of the policy and rules.

6. A requirement that written consent to the school district policies must be obtained from the community users. Users can waive their rights to privacy through consent, allowing district access and monitoring of e-mail and other Internet usage. The district has a right to act in good faith to uphold a legitimate interest or duty, such as ensuring the lawful use of school property and the protection of minors from harmful materials.