



JANUARY 2004

A PRACTITIONERS BULLETIN

## A Principal's Guide to Internet Policies & Electronic Communication

By Brian D. Schwartz, Dr. Larry Janes and Kenneth Reed

### I. Introduction:

With the advent of the Internet and computer technology, today's students enjoy access to every corner of the globe. Communications that once took weeks are now literally instantaneous. It is a world far different from the one most school administrators grew up in. In most cases, it is an area where the knowledge of students far exceeds that of teachers, administrators and school board members.

**Editor's Note:** This article is reprinted with permission from the National Association of Secondary School Principals. This article originally appeared in the winter 2004 edition of NASSP's "A Legal Memorandum."

By: **Brian D. Schwartz**, General Counsel, Illinois Principals Association and Adjunct Professor of School Law, Southern Illinois University at Edwardsville

**Dr. Larry Janes**, Professor Emeritus, Eastern Illinois University and Educational Consultant

**Kenneth Reed**, Director of Technology, Champaign (Illinois) C.U.S.D. #4 and Technology Coordinator to the Illinois Principals Association Board of Directors

However, it is imperative that school officials, especially school administrators, keep up to date on the latest developments in technology. Although the Internet is an invaluable research and learning tool, there is a tremendous responsibility on schools to scrutinize how students and staff use school computers and e-mail systems. Each day seems to bring new regulations and lawsuits, as legislatures and courts try to keep pace with technology.

The purpose of this article is to bring school administrators up to date on the legal and practical aspects of monitoring and regulating computer use within the schoolhouse gates. The material below takes a detailed look at the ability of schools and school districts to regulate the use of school computers and electronic communications by both students and staff members and the duty to safeguard school records and property that are stored via computer databases.

### II. Schools, Websites and Electronic Communications:

#### a. The Ability to Regulate School Websites

Schools enjoy a great deal of authority when it comes to regulating school created and maintained websites. If the website is indeed solely maintained by the school or district, a closed forum may be created, whereby the website may be used solely for school purposes. (See,

*e.g.*, *Hazelwood School District v. Kuhlmeier*, 484 U.S. 260 (1988) (a school enjoys full editorial control over a school-maintained and sponsored student newspaper). However, much like the use of a school's grounds and facilities, a school may open up the use of its website to non-school related groups and to the public.

Once a school decides to open its website to use by outside groups, all similarly situated groups must be granted the same opportunities. For example, if a school allows a local civic group to post an event announcement to the school's website, all other community groups, whether or not they comport with the school's educational mission, must be allowed to post announcements for their events. (See, *e.g.*, *Good News Club v. Milford Central School*, 533 U.S. 98 (2001) (once a school opened its doors to local community groups, a local religious group could not be denied use of the school's facilities) and *Perry Ed. Assn. v. Perry Local Educators' Assn.*, 460 U.S. 37 (1983) (when a school allowed one union access to the teachers' mailboxes, all other unions must also be granted similar access).

Additionally, the federal Equal Access Act provides that student religious organizations must be granted the same access to school facilities as other student organizations, unless the school specifically limits access only to curriculum related student organizations. (20 U.S.C. 4071). The same principals un-

doubtedly apply to school website use by student groups.

In light of the above discussion, schools would be wise to specifically delineate their policy for school website use. Schools may limit the use of the school's website to school related materials and events (creating a closed forum), limit the school website to use by student groups (creating a limited-open forum) or allow the website to be used by all community groups (creating an open public forum). Additionally, consistent with the *Hazelwood* decision, students should be told that the school has final editorial authority whenever students are given school credit for designing, editing or updating the school's website.

### **b. The Constitutionality of Internet Filtering Software**

The use of Internet filters is one of the most hotly debated topics in the area of technology law. The main debate focuses on whether such filtering mechanisms are a form of censorship and undermine constitutionally protected free speech.

The filter debate has been fueled by the federal Children's Internet Protection Act (CIPA), which requires that, as a condition of receiving certain federal funds, public school districts and libraries have filtering software on all computers by July 1, 2002. (Public Law 106-554, codified at 20 U.S.C. 3601, 20 U.S.C. 9134 and 47 U.S.C. 254(h)). The Act was recently challenged as it applies to public libraries, and was initially held to be an unconstitutional infringement on the First Amendment. However, on June 23, 2003, the United States Supreme Court reinstated the Act as it applies to public libraries. The Court stated that in order to fulfill their educational and cultural roles, libraries must have broad discretion to decide what materials to provide to their patrons. Also key to the high Court's 6 to 3 decision was the fact that the filters could easily be disabled for research and other legitimate purposes. (*United States v. American Library Association, Inc.*, \_\_\_ U.S. \_\_\_,

Docket No. 02-361 (2003)).

The Children's Internet Protection Act has never been challenged as it applies to public schools. However, the Supreme Court's *American Library Association* decision would seem to invalidate any remaining questions of the Act's constitutionality as it applies to educational facilities. Like libraries, the mission of public schools is primarily one of education. Just as libraries choose not to make every book available to patrons in order to keep with their mission, schools must meet similar educational obligations to their students.

Public schools seem to have even more authority to restrict content on computers that are located within the classroom. In a 1982 case, the United States Supreme Court ruled that school officials may not remove books from a public school's library simply because they find the books distasteful or dislike the message contained therein. However, the Court took great care to distinguish the relative openness of school libraries as compared to the classroom, where school officials enjoy almost complete authority to regulate curriculum. (*Board of Education, Island Trees Union Free School District No. 26 v. Pico*, 457 U.S. 853 (1982)).

At the same time in which schools are subject to lawsuits for censorship, others have been under scrutiny for failing to protect children from the harmful effects of the Internet. In light of the current debate on Internet filters, one might ask how schools might meet their obligation to protect students from harmful information found in cyberspace, while at the same time keep from violating First Amendment guarantees. The following tips are designed to assist school officials in maintaining adequate security and preserving student rights:

1. Internet filters are not a substitute for schools diligently monitoring student computer and Internet use. Students should always be appropriately monitored to make sure they are complying with the school's

Acceptable Use Policy and other school rules.

2. When filters are used, the school should develop a filtering policy that is tied to student safety and the Children's Internet Protection Act. It is essential that all school policies are elucidated before they are challenged.
3. School personnel should be given flexibility to determine what Internet material is offensive given the age of the students and other appropriate standards.
4. All filtering devices should have a mechanism to disable the filtering software for bona fide research or other lawful purpose, provided the student or staff member has prior permission from the appropriate administrator.

### **c. File-Sharing**

File-sharing programs allow people to share files with others on the Internet. Although the concept of being able to share files on the Internet is a noble one, the process and the content involved in file-sharing have many pitfalls for schools. To understand the pitfalls that file-sharing holds for schools, it is important to know more about how the file-sharing programs operate.

A number of software programs are available that facilitate the file-share process, such as Kazaa, Morpheus, Limewire and WinMX, to mention a few. If a student, or staff member, loads a file-sharing software program on a school computer, it allows the user and the other clients that are a part of the file-sharing network to access all files that are resident on the file-sharing network's computers. It also allows the file-sharing network to utilize the client's computer to help run the file-sharing network, significantly degrading the function of the overall local area network due to the Internet traffic that file-sharing creates.

Secondary considerations related to file-sharing involve the appropriateness

of content of the file-sharing and copyright considerations related to that content. File-sharing, depending on the configuration of your network, may allow for inappropriate material to be downloaded or accessed by students or staff. In addition some file-sharing downloads may be an infringement of copyright laws that could result in financial penalties for the school district.

To guard against the pitfalls of file-sharing, schools need to take preemptive steps. File-sharing by students and staff should not be allowed, as explicitly stated in the district's acceptable use policy. A school district's local area networks (LANs) should be equipped with software that monitors Internet traffic to detect any file-sharing within the LAN. Finally, school district policy should address software file-sharing downloads and copyright violations.

#### **d. FERPA and Confidentiality**

The creators of the federal Family Educational Rights and Privacy Act, or FERPA, most certainly never contemplated the advent of cyberspace. (20

must carefully examine the method in which they store electronic records. Such records should be protected with a password and only those individuals with a need to know should be allowed access. Additionally, schools should be aware that a student record may be created when a student visits a website using a school computer. Often times an individual transmits personally identifiable information to the website owner simply by visiting a site. To date, federal officials have not issued any guidelines on how to address this situation. (Howie, Margaret-Ann F., *The Legal Connection: Navigating Technology Issues in Your Schools*, 1:13, LRP Publications, 2001).

Also under FERPA, schools may release certain directory-type information to the public without parental consent. Such directory information generally includes a student's name, address, telephone number and field of study. (20 U.S.C. 1232g(5)(A)). However, schools should take great care when posting directory information to the school's website. As compared to a newspaper,

AUP for your school or district:

1. Scope of Use: Each school or district must determine what scope of use it will allow for students and staff. Most districts do not allow either students or staff to have unlimited access to the World Wide Web and include a statement in their AUP that Internet and e-mail are solely for educational purposes.
2. Rules for Usage: Any good AUP for both staff and students states that Internet and e-mail use is a privilege and not a right, and that a violation of the AUP may result in termination of usage and/or appropriate discipline. The school's rules should also be clearly listed so as to provide adequate notice. Additionally the appropriate discipline policy should be incorporated by reference so as to allow the school the full range of disciplinary options.
3. Prohibited Uses: The AUP should contain a statement that the school condemns any illegal use of the school's computer system, including the pirating of software, hacking, copyright violations, harassment or threats, defamation and the like. Schools are also wise to consider the following prohibited activities: use of obscenities, viewing or downloading pornographic materials, sharing account information or attempting to use another person's account, file-sharing or downloading file-sharing programs, harming school property, attempting to bypass or bypassing the school's filtering system or participating in any other activity that is detrimental to students, the school or school officials.
4. Liability: The AUP should include a provision that the school does not guarantee the

*AUPs serve not only to protect schools from liability, but place students and staff on notice as to rules, regulations and expected conduct.*

U.S.C. 1232g). However, the Act's impact on the storage and maintenance of student records is enormous. Essentially, FERPA provides that, with limited exceptions, student records must be kept strictly confidential and can only be released to individuals with a legitimate educational interest unless a child's parent otherwise consents. Student record is further defined as any document that personally identifies a student and is maintained by the school, no matter where that record is stored. (20 U.S.C. 1232g(4)(A)).

Given the above definition of student record, schools and school districts

which is primarily local in nature, information on the World Wide Web can be accessed by any person at any time.

### **III. Guidelines for Acceptable Use Policies:**

Acceptable Use Policies, or AUPs, are an important element of any school's technology planning. AUPs serve not only to protect schools from liability, but place students and staff on notice as to rules, regulations and expected conduct. AUPs differ dramatically in their scope and depth. Listed below are essential considerations in the development of an

reliability of the data connection and does not verify the accuracy of information found on the World Wide Web.

5. **Property/Privacy Statement:** A statement should be included in the AUP that all information sent or received from a school computer, including e-mail, are school district property, should not be considered confidential and may be accessed by school personnel at any time.
6. **Training Sessions:** Some schools have experimented with mandatory training sessions for both students and staff before allowed access to the Internet or assignment an e-mail address.
7. **Agreement Provision:** It is recommended that both students and staff sign a document indicating that they have read and understand the appropriate AUP and agree to abide by the terms and conditions contained therein. Students and staff should also agree in writing to indemnify the school or district against any losses or damages that occur out of violations of the AUP.
8. **Parent Permission Form for Student Use:** Many schools also require parent approval before students are allowed to use the Internet or the school's e-mail system. It is recommended that any parental permission slip also contain a statement whereby the parent agrees not to hold the school, district or school personnel responsible for any material the student accesses or transmits via the school's computer system. (See, *in part*, Dipietro, Rosann, *School Laws in Massachusetts*, Exhibit 10A, Mass. Continuing Legal Education, Inc., 2003).

## IV. Student and Staff E-Mail Use:

### a. E-Mail Use In General

A growing number of students and school staff members have electronic mail or e-mail addresses that are routed through the school or district's technology network. Furthermore, many students and staff members are able to access their respective e-mail accounts from home computers or other computers that are off of school property. This use of e-mail has created two primary concerns for schools and school districts: user privacy and sexual harassment through the school or district's e-mail server.

### b. User Privacy and the Electronic Communication Privacy Act

Any discussion of e-mail privacy in schools starts with the Electronic Communications Privacy Act, or ECPA. Adopted in 1986, the Act is part of the federal wiretapping statutes and deals with the way schools and other entities monitor electronic mail. (18 U.S.C. 2510, *et. seq.*). Specifically, the Act makes it a criminal offense to intercept electronic mail while such mail is in transit.

There have been at least two important federal appellate court decisions that have provided clarity to the Act as it applies to schools. In *Steve Jackson Games, Inc. v. U.S. Secret Service*, the fifth district appellate court held that Congress did not intend for "intercept" under the Federal Wiretap Act to apply to "electronic communication" when those communications are in "electronic storage" within the provider's system. (36 F.3d 457 (5th Cir. 1994)). Additionally, in *Pollock v. Pollock*, the sixth federal circuit held that as long as a parent or guardian has a good faith basis for believing that it is in the best interest of the child, the parent or guardian may vicariously consent on behalf of the child to the recording of a telephone conversation. (154 F.3d 601 (6th Cir. 1998)). Many school law experts believe that the *Pollock* decision would naturally extend to student e-mail.

However, despite the latitude granted to school officials in viewing staff and student e-mail, students and especially staff may still have a reasonable expectation of privacy in their e-mail communications. (See, *e.g.*, *O'Connor v. Ortega*, 480 U.S. 709 (1987) and *Vega-Rodriguez v. United States v. Simons*, 29 F. Supp. 2d 324 (E.D. Va. 1998) (both discussing employee Fourth Amendment rights in the workplace of a public employer). Therefore, schools are wise to take the following steps: clearly outline that there is no expectation of privacy in e-mail communications that are accessed or delivered through the school or district network, allow school officials to access e-mail communications at any time and limit e-mail use to school purposes. These steps are most effectively taken through the acceptable use policy. Staff members and students (along with their parents) should always sign a copy of the AUP or documentation acknowledging the aforementioned privacy waiver.

### c. Sexual Harassment through E-mail

Schools and school districts have seen increased liability in the cases of employer to employee, employee to student and student to student sexual harassment. The use of e-mail has provided another avenue for sexual harassment and has increased the responsibility of educational institutions to deal with this problem.

Most cases of sexual harassment against schools and districts are brought in federal court under either Title VII of the Civil Rights Act of 1964 or Title IX of Educational Amendments of 1972. Title VII provides, in part, that it is unlawful to discriminate against someone in an employment capacity because of the person's race, color, religion, sex or national origin. (42 U.S.C. 2000e-2). This statute protects employees from sexual harassment from supervisors or other employees. In order for a district to incur liability, the victim of the harassment must show that the harassment was done under the guise of employment and that the district knew about the situa-

tion - or should have known - and failed to take reasonable action. (*See, Faragher v. City of Boca Raton*, 524 U.S. 775 (1998)).

Title IX protects students and provides, in part, that no person on the basis of sex may be denied the benefits of or participation in the educational process. (20 U.S.C. 1681). In order for liability to ensue against the school or district, the victim must show that the sexual harassment was objectively offensive, that the school or district had actual knowledge of the situation and that the school or district acted with deliberate indifference in failing to diffuse the situation. (*See, Davis v. Monroe County BOE*, 526 U.S. 629 (1999) and *Gebser v. Lago Vista Ind. School District*, 524 U.S. 274 (1998)).

In lawsuits brought under either Title VII or Title IX, the law imposes on the victim the burden of proof. What constitutes constructive or actual notice by the school or district is frequently a subject of litigation. Written e-mail communications presented to school officials may aid in establishing such notice, whether actual or constructive. The victim's continued receipt of such harassing e-mail through the school or district's network may further establish that the school or district failed to take the appropriate action. (Conn, Kathleen and Zirkel, Perry A., *Legal Aspects of Internet Accessibility and Use in K-12 Public Schools: What Do School Districts Need to Know?*, 146 Ed. Law Rep. 1, 27, West Publishing, 2000).

## V. Discipline for Computer Misuse:

### a. Discipline for Misuse of School Computers

As discussed above, schools generally enjoy the ability to fully regulate the use of school computers. Schools must, however, take care to assure the right to discipline students and staff for misuse of school computers. The AUP should specifically state that the use of school computers is a privilege – not a right.

Prohibited uses should be specifically spelled out and the appropriate disciplinary policies should be incorporated by reference.

### b. Home-Based Websites and Discipline

Perhaps the most difficult area of technology law is the ability of schools to discipline a student or staff member when that individual uses their home computer to disparage the school or convey threats to students, staff or school officials. Students and staff certainly have increased First Amendment rights when using home computers, but these rights are not without limitations.

In order to discipline a student or staff member for speech conveyed on their home computer, three elements must be present: (1) there must be a connection or relation-back to the school, (2) the student or staff member's actions must have violated a legitimate school policy or law, and (3) the school must, after a thorough investigation, show a substantial disruption to the educational process or a legitimate safety concern.

The courts have addressed several cases dealing with off-campus discipline of students. In *Beussink v. Woodland R-IV School District*, a student developed a home website that referred to school staff in vulgar terms and invited viewers to express their own thoughts regarding the school. Using the "material and substantial disruption test" elucidated in *Tinker v. Des Moines Independent School District*, the court found that the school's discipline of the student violated his First Amendment rights. Specifically, the court held that school officials overreacted and that displeasure with content, absent more, is not enough to impose discipline. (30 F. Supp. 2d 1175 (E.D. Mo. 1998); *see also, Emmett v. Kent School District NO. 415*, 92 F. Supp. 2d 1088 (W.D. Wash. 2000) (holding that absent an actual threat, a school could not impose discipline against a student for comments on his home website).

However, in *J.S. v. Bethlehem Area School District*, a court upheld the

school's discipline of a student who solicited donations to kill a teacher via his home-based website. The court found that the school had fully investigated the matter, the student violated clearly posted school rules and there was a substantial disruption of the school's operations based on the threats. (757 A. 2d 412 (Pa. 2000)).

The above cases clearly indicate that schools have limited authority to discipline individuals for off-campus use of home computers. Other ideas to control conduct include: notifying parents in the case of students, contacting the Internet Service Provider (ISP) to determine if the conduct violates the ISP agreement, contacting local law enforcement to see if the conduct violates community decency laws and encouraging the aggrieved party to institute a civil lawsuit against the offender.

## VI. A Word on Copyright Law:

Although a complete discussion of copyright law is beyond the scope of this article, there are a few comments that should be noted regarding student and school use of copyrighted material from a digital medium perspective. Copyright law extends to all original works of authorship, including software programs, CD-ROM and web pages. Additionally, it is no longer required that an author place notice on the document or register it in order to receive all of the rights enumerated by the federal Copyright Act. (17 U.S.C. 101, *et. seq.*).

There are two important exceptions to the Copyright Act as it applies to the educational setting. The fair use doctrine provides that the "the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright." There are four specific factors to be applied in determining whether or not a particular use violates copyright law: (1) the purpose and character of the use, including whether such use is of a

# Illinois Principals Association

2940 Baker Drive • Springfield, Illinois 62703 • 217-525-1383  
*Dedicated to Improvement of Elementary and Secondary Education*

commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. (17 U.S.C. 107).

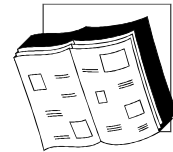
Public schools also benefit from three exemptions under the copyright law: face-to-face teaching at nonprofit educational institutions, educational broadcasting and not-for-profit performances. In the first exception, instructors may generally read, perform or display copyrighted material in a face-to-face address. Instructional broadcasting allows the performance of a

non-dramatic literary or musical work for instructional purposes. Non-profit performances allows for the non-public performance of non-dramatic literary or musical works that are not for monetary gain. (17 U.S.C. 110).

Schools would be wise to adopt a formal policy warning students and staff of the general guidelines under the Copyright Act and the consequences for illegal use of copyrighted material. For an excellent discussion of copyright law, consult Darden, Edwin C., ed., *Legal Issues & Educational Technology: A School Leader's Guide*, 2<sup>nd</sup> Edition, Chapter 4, National Association of School Boards, 2001.

## VII. Conclusion:

It is the authors' hope that the above article is helpful in communicating to school officials some of the most important areas of schoolhouse technology. In closing, please note that the above material primarily takes into account federal law and national trends. Your specific state may have additional laws or regulations that must be considered. Additionally, it is important to consult with your school attorney or legal advisor before taking final action with respect to any policy or practice within your school district.



Return Service Requested

