The following document is from:

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

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

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



# *Part II. Safe and Responsible Internet Use Plan*

# *7. Supervision, Monitoring, and Privacy*

## CIPA Requirements

The CIPA requirements related to monitoring are:

> CERTIFICATION WITH RESPECT TO MINORS.-- A certification under this paragraph is a certification that the school, school board, local education agency, or other authority with responsibility for administration of the school--
>
> (i) is enforcing a policy of Internet safety for minors that includes monitoring the online activities of minors[1].

[1] 47 U.S.C. 254 (h)(5)(B).

Neither the CIPA statute nor the FCC regulations provide a definition for the term "monitoring." Common use of the term monitoring includes the concepts of in-person staff supervision, the use of "real-time" monitoring devices that allow for the distant viewing of computer terminals, and staff or technical review of Internet usage records.

A reasonable presumption is that to comply with CIPA, districts must enforce a policy that includes a good faith effort to engage in an appropriate level of monitoring to protect against access to material that is considered potentially harmful. Most districts use a combination of supervision or "real-time" monitoring and a periodic analysis of Internet usage records.

There is no requirement in CIPA that the activities of adults using a district Internet system be monitored. But clearly, the district will want to ensure that staff is not misusing the Internet and, therefore, staff use should also be monitored.

## Remaining "Hands-On"

The essential component of supervision and monitoring is the removal of the perception of invisibility. Supervision and monitoring is the way in which educators remain "hands-on" -- knowing where students are, what they are doing, and who they are doing it with. When young people are in an environment where adults have remained "hands-on" they are much less likely to engage in risk-taking or inappropriate behavior.

For the purposes of this document, supervision will refer to "real time" activities where school staff are present and attentive to student Internet use as it occurs. Monitoring will refer to analysis of student use that occurs after-the-fact or using technical systems that allow for the review of student use outside of the physical presence of the students. Both supervision and monitoring can be facilitated through the use of technology. Real-time systems can provide the ability for a staff person to view the screens of remote computer. Technologies can also filter and review Internet usage traffic and identify traffic that is suspected to be in violation of the district policy, as configured into the monitoring technology.

The *NRC Report* specifically addressed the issue of privacy in the context of the use of technical monitoring in schools.

> (T)he level of privacy that students can expect in school -- using a computer as well as in other aspects of school life -- is different from what they can expect at home, and school computer systems are not private systems. The expectation of privacy when students use computers in schools is more limited, as is evidenced by a variety of actions that have been supported in court decisions, including searches of student lockers, backpacks, and so on. Thus provided that students have been given notice that their use is subject to monitoring, the use of monitoring systems raises fewer privacy concerns[2]

[2] National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002). URL: http://bob.nap.edu/html/youth_internet/. at Section 12.2.5.

***Supervision***

Supervision requirements should be appropriate to the age and circumstances of the students. The supervision requirements for a class of elementary students, will be different from the requirements for high school staff of the school newspaper. Supervision requirements will likely also be different for different groups of students within one school. Educators generally have a good sense of the abilities, aptitudes, and inclinations of their students, including their ability to make safe and responsible choices in their use of the Internet.

It is recommended that the district policy include reference to supervision requirements related to the age and circumstances of the students, with a delegation to school administrators to further define and delineate the supervision requirements and expectations for their schools. The staff that are supervision student use of the Internet in environments or at times when students use is not restricted to specific class-related activities should receive professional development related to issues of students' rights of access to information. Staff may not restrict student access to certain information or sites based on the staff member's views of what is or is not appropriate information. Such decisions should be made in accord with the standards set forth in district policy.

To facilitate effective supervision also requires consideration of the physical placement of computers. To the greatest degree possible all computers that are used by students should be positioned in a way so that the screen is clearly visible to others. Stores that sell X-rated merchandise generally have driveways that are screened and windows that are boarded up. There is a reason for this. The more publicly visible the activity, the less likelihood there is for the demonstration of questionable behavior. As school administrators review the supervision requirements for their school, an analysis of the placement of the computers would also be advisable.

Under the approach set forth in this Guide, students in elementary school will have access to the Internet in an environment that generally limits their use to access to pre-reviewed and approved web sites. There may, however, be occasions where access to the more open Internet is necessary to achieve a specific educational purpose. If elementary students have access to the more open Internet, staff should provide close "over-the-shoulder" supervision.

For secondary students, effective supervision and monitoring is the critical strategy to address concerns of irresponsible or unsafe behavior. Effective supervision and monitoring allows students to have more freedom in their use of the Internet and places the responsibility squarely on their shoulders to exercise that freedom in an appropriate manner.

Secondary schools may also consider the use of student lab monitors to provide additional supervisory capacity. Students who have been granted such authority tend to take their jobs very seriously. They consider misuse by other students to reflect badly on the entire student body. Student supervisors are also very likely to be in tune with behavioral clues that other students may exhibit if involved in misuse.

### *Monitoring*

Effective monitoring of Internet usage will help to identify instances of inappropriate or unsafe use that may have been undetected notwithstanding appropriate supervision. The implementation of an effective monitoring system is an excellent measure to prevent problems. When students know that they are leaving little "cyberfootprints" that can easily be tracked by the system administrator, they are much less likely to even think of doing something that will result in detection and discipline.

To ensure effective monitoring, secondary students should be provided with a unique student user ID. Many schools follow a practice whereby students may only receive this user ID upon completion of an Internet Use Policy class. The use of a unique student user ID should not be necessary at the elementary level because the focus at this level of schooling is protection in safe Internet spaces.

Real-time monitoring can occur through the use of monitoring technologies that allow the lab supervisor to remotely view any of the computer screens in the computer lab, or school. After-the-fact monitoring involves an analysis of student usage records and files. In smaller districts with a low level of Internet traffic, periodic staff analysis of Internet usage records may be sufficient. However, with larger districts, staff analysis will be too time-consuming. Districts may want to consider the acquisition of a technology tool to provide assistance with the monitoring.

There are newer filtered monitoring technologies coming onto the market provide an excellent monitoring capability. These technologies use a packet-sniffing technology and linguistic analysis to filter all Internet traffic, including not only web sites, but also e-mail and any real-time communication activities. The packet sniffing technology will report cases of suspected violations of the District Internet Use Policy. Administrators can then review the reported usage to determine whether there was an actual violation. For example, a report may reveal that a student accessed one site with pornography but exited that site within 5 seconds -- clearly indications of mistaken access. But a student will have difficulty arguing that he or she mistakenly accessed a site with pornography when the report indicates that the student was viewing the site for 3 minutes, and then accessed several more pages on that site.

## Student and Staff Privacy Issues

### *Legal Standards*

Monitoring student and staff use of the Internet in schools necessarily raises the issue of legal standards related to student and staff privacy. Most of the case law related to privacy issues has emerged in the context of criminal cases and have related to an interpretation of the Fourth Amendment restrictions on search and seizure. This case law has also be interpreted in the context of searches of student or staff personal belongings in school.

The initial analysis in such cases relates to the expectation of privacy. The United States Supreme Court in *Katz v. United States* first enunciated the constitutional standards related to

expectations of privacy and established a two-part test[3]. The first part of the test requires "[t]he person must have had an actual or subjective expectation of privacy.[4]" The second part requires that this subjective "expectation be one that society is prepared to recognize as 'reasonable.'[5]" If these two tests are satisfied, then there is said to be a "reasonable expectation of privacy."

There are two additional doctrines that have emerged in this area that appear to be relevant. The first is the plain view doctrine. Under the plain view doctrine, if a public official who is legitimately where he or she is able to be, sees something in plain view, there are no privacy protections. The second doctrine is that of consent. In *United States v. Simons*, government agency network services administrator found patterns of use that indicated that an employee was accessing Internet pornographic material. Further search was made of the employee's computer and a significant number of pornographic files were found. The employee objected to the search on Fourth Amendment grounds. The court upheld the search, indicating that the government agency's policy on computer use indicated the potential of audits of web usage to identify instances of inappropriate activity.

The standards for school officials in conducting a search and seizure of a student in the school setting where there is a legitimate expectation of privacy were enunciated by the Supreme Court in the case of *New Jersey v. T.L.O*[6]. These standards are:

- Was the search "justified in its inception[7]?" A search is justified when there are "reasonable grounds for suspecting that the search would turn up evidence that the students has violated or is violating either the law or rules of the school[8].

- Was the search "reasonably related in scope to the circumstances which justified the interference in the first place[9]?" A search is reasonable when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction[10]."

The extent of a district's ability to investigate the personal files of staff is less clear. In *O'Connor v. Ortega*[11], the Supreme Court held that employees did have constitutionally protected privacy interests in the work environment but that the reasonableness of the employee's expectation of privacy must be determined on a case-by-case basis. The Court then applied the *T.L.O.* standards of reasonableness to employer intrusions of employee privacy for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct.

### *Application of Legal Standards to Internet Use in Schools*

---

[3] *Katz v. United States*, 389 U.S. 347 (1967) The two-part test was first enunciated in Justice Harlan's concurring opinion and subsequently applied in other Fourth Amendment cases. e.g., *Smith v. Maryland*, 442 U.S. 735, 740-41 (1979)
[4] *Id.* at 350-52, 360.
[5] *Id.* at 361 (Harlan, J., concurring).
[6] 469 U.S. 325 (1985).
[7] *Id.* at 341.
[8] *Id.* at 342 (citations omitted).
[9] *Id.* at 342.
[10] *Id.* at 342 (citations omitted).
[11] 480 U.S. 709 (1987).

**Expectations of Privacy**
Based on the above standards, let's now consider the situation related to Internet use in schools. Many school districts have a policy that reads something like. "There are no expectations of privacy in the use of the Internet."

What does this mean?

- Does this mean that any teacher can, at any time, review the web usage records and e-mail files of any other staff member or student?

- Does this mean the superintendent can regularly review the e-mail messages of staff union leaders?

- If a group of students are working to establish a chapter of the Gay, Lesbian, Straight Education Network at school, can the building principal who objects to the establishing of this organization request access to the web usage logs and e-mail files of these students?

Regardless of the statement in the district policy, it is likely that the vast majority of people would not be comfortable with the above intrusions into Internet records.

*On the other hand*, when students are using the Internet in a computer lab, there is very little privacy because much of what they are doing is in plain view.

*On the other hand*, if there is no expectation of privacy, then how is it that users are asked to establish a password for access to their personal files and warned to keep that password private?

*On the other hand*, there appears to be a higher expectation of privacy in a person's e-mail files as compared to records of web searches. This may be because just about everyone knows that web usage is being tracked by different entities for different purposes, whereas the contents of e-mail messages are not so publicly available. This may be because of the nature of personal communication, rather that information searching. Essentially, the rationale for this perception is unknown.

*On the other hand*, electronic communications of public employees are generally considered to be discoverable under state public records laws, therefore it could be argued that employees have no expectation of privacy.

*On the other hand*, the common practice is to treat staff e-mail as private.

In other words, there are a lot of "*on the other hands*" in this situation -- meaning that despite a clear statement in a policy, there remains an expectation on the part of many users of a district system that there is, at least, some level of privacy in their use of the Internet at school.

**Locker Search Standard**
Looking at the situation from a different angle, it would be recognized that most school districts have students search and seizure policies related to student lockers and desks that are in accord

with the *T.L.O.* legal standards. The policies provide that a general inspection may occur on a regular basis, with advance notice to the students. Special inspections of individual lockers or desks may be conducted when there is reasonable suspicion to believe that illegal or dangerous items or items that are evidence of a violation of the law or school rules are contained in the locker or desk. These same standards can be applied in the context of analysis of Internet usage records and e-mail files.

To further explore this issue, the author raised this topic for discussion on an e-mail discussion list. Several respondents indicated that their district policy was that there was no privacy. Then the author presented scenarios such as those above and pressed the respondents to further explore the issue. In every case, the basic desired standard that emerged through the discussion was a version of the locker and desk standard.

Essentially, there appears to be a basic underlying perception of a limited expectation of privacy in schools. The underlying expectations appear to be different for web usage logs, as compared to e-mail files. It is acknowledged that the district must regularly review web usage logs. It is not generally not anticipated that the district will regularly investigate personal e-mail files. An exception to this is in elementary school, where students using a classroom account have no expectation of privacy.

Further, it appears that it is considered to be appropriate for the school district to investigate personal files -- including an analysis of a individual user's web usage logs or their personal e-mail files, if, and only if, there is a reason to believe that the user has engaged or is engaging in inappropriate activity. Essentially, this is the "reasonable suspicion" standard.

The following is the outline of the manner in which the standard school locker and desk search standards can be applied in the context of Internet usage.

**Routine Monitoring**
Users should be provided with a notice that all use of the Internet will be monitored on a regular basis.

Some districts may opt for staff monitoring of web logs and other usage data. This approach is feasible with a smaller district with low amounts of Internet usage. For larger districts, the staff monitoring activity may become unnecessarily time consuming and/or ineffective.

Routine monitoring may be facilitated with the use of technical monitoring tools. These tools may operate in "real time," such as monitoring systems that allow an administrator to directly remotely view what is on the screen of another computer. Filtered monitoring technologies utilize an intelligent analysis of Internet use traffic that seeks to detect communication patterns that may reveal instances of inappropriate activity.

**Individualized Searches**
Special inspection of the online activities of an individual user would occur when there are indicators that raise a reasonable suspicion that inappropriate activity has or is occurring.

The district should establish a process by which individualized searches are considered appropriate. Any individualized search of student e-mail files should be conducted only by authorized staff. Generally, the staff that are authorized to conduct an individualized searches will be the district's technology director, his/her designee, and administrators in the students' school.

Filtered monitoring technologies that analyze Internet usage and report on activity that is suspected to be in violation of the policy work in a manner that would meet the reasonable suspicion standard. They report on activity that is suspected to be in violation of the district's policy or the law, based on parameters established by the district. An individualized search can verify whether or not the reported suspected misuse is actual misuse or not. Internet usage traffic that does not raise concerns of possible misuse remains private.

**Instances Where There are No Expectations of Privacy**
There also may be situations where there are no expectations of privacy. These situations may include the following:

- Elementary students using electronic communications should likely have no expectations of privacy. They should use group or classroom e-mail accounts. If individual e-mail accounts are established, teachers should have full and complete access to these accounts at any time for any reason.

- The elimination of any expectation of privacy may be an appropriate disciplinary response when a student has been misusing electronic communications. As a disciplinary consequence, a student can be informed that for a period of time an administrator can and will regularly review his/her personal e-mail files or the e-mail system can be configured to have an automatic copy of any communication by the student sent to the teacher.

- If there are significant problems emerging within a particular school related to electronic communications, the school administrator may decide that for a period of time there will be absolutely no expectation of privacy and any and all student personal e-mail files may be reviewed at any time.

- There is no expectation of privacy for students in the event their parent requests access to their Internet usage files.

- There is no expectation of privacy, in the event of a public records request, except as provided under the state's public records laws.

**Staff Privacy**
The district policies related to staff privacy should likely also be addressed in collective bargaining agreements. In many cases, the standards for special inspections of staff classrooms or desks are similar to those set forth in student policies, that is, desks and classrooms may be searched if there is reasonable suspicion that the staff member is violating a law or school policy. Collective bargaining agreements also generally contain provisions regarding documentation of

any individualized searches. These policies and agreements should be reviewed to determine their applicability to Internet searches.

***NOTICE!***

*The most important* step a district must take is fully and completely informing all students and staff what they can expect in terms of privacy.

All users of the system should be provided with absolutely clear notice about how the district will monitor Internet use. If any technology monitoring tools are used, secondary students and staff should be provided with records of how the system works and what evidence it can detect. Districts may want to remind students of the monitoring with a notices and examples of usage records placed in computer labs. Some districts provide information about the limitations of privacy directly on the log-on screen so users are reminded of monitoring every time they log onto the computer.

The most important reason to provide effective notice is the preventive effect of such notice. Providing students with demonstrations of how the district's monitoring strategy or system identified misuse can act as an effective deterrent to future misuse. When students are fully aware of how their actions are being monitored, only the most foolish will risk engaging in misuse.

The following is an example of policy language that can be used to specifically address student and staff privacy in the use of the Internet that will provide adequate notice:

> "Users have a limited expectation of privacy in the contents of their personal files, communication files, and record of web research activities on the district's Internet system. Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead to discovery that a user has violated district policy or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated district policy or the law. Students' parents have the right to request to see the contents of their children's files and records. Staff are reminded that their communications are subject to Freedom of Information laws."

Districts can provide ongoing notice of by providing a notice as part of the computer log-on screen in a manner such as follows:

> "The district's computer and Internet system is to be used for educational purposes. Users are reminded that all Internet use is monitored by the district."

## Addressing Expectations of Privacy

People are still struggling to hold onto the right of privacy at the same time that technology seems to be removing many vestiges of this important interest. It is reasonable for districts to expect concerns to be raised regarding intrusions into privacy and to provide a rationale for the manner in which the district intends to monitor student use of the Internet.

The basis of this rationale is learning to distinguish when and where we can and should expect privacy and when and where we should not expect privacy -- and then to govern our behavior and communications based on that expectation. For example, students who discuss private matters in the middle of a crowded lunch room are in no position to complain about the violation of their personal privacy on the part of those who might overhear their conversation.

School districts have an obligation to protect the safety of students when they are using the Internet and to ensure that the district's Internet resources are being used responsibly. The district cannot meet this obligation without engaging in supervision and monitoring. Therefore expectations of privacy must be guided by an understanding of the limitations of privacy when using the district's Internet system.

Further, districts must prepare students to be successful in their future work environments. The vast majority of employers, both corporate and government, are regularly monitoring employee use of the Internet, including web logs and e-mail. Therefore, it is appropriate for students to learn how to manage their behavior on monitored Internet systems.