

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 29<sup>th</sup> Avenue  
Eugene, Oregon 97405  
541-344-9125  
541-344-1481 (fax)  
Web Site: <http://responsiblenetizen.org>  
E-mail: [info@responsiblenetizen.org](mailto:info@responsiblenetizen.org)

Copyright © 2002-03 Nancy E. Willard. This document is distributed as "Honor Text."

The purpose of the "Honor Text" approach is to allow for the wide dissemination of information, while providing financial support for continued policy research and dissemination. The following are the "honor text" guidelines:

- If you are a student or other researcher and are using one copy of this material for personal research, you are not requested to provide compensation.
- If you have established a web site or web page listing information resources for educators, you may freely link to this site or any individual document on this site and are not requested to provide compensation.
- If you are a faculty member, professional development coordinator, or the like and have assigned material on this site as readings for your students (whether provided in hard copy or linked to as an online component of course resources), you are requested to provide compensation for such use. The standard rate for the reproduction of copyrighted materials for courses is \$.10/page/student. If you are using substantial sections, please make contact to arrange for discounts.
- If you are a school or a district and have used these materials for planning and/or policy development, you are requested to provide compensation in a manner that reflects the perceived value.
- For all other uses or further information, please e-mail us at [info@responsiblenetizen.org](mailto:info@responsiblenetizen.org).

Although the author has made every effort to ensure the accuracy and completeness of the information contained in this book, the author assumes no responsibilities for inaccuracies or omissions. Although this book discusses legal issues, nothing contained in this book should be interpreted as the provision of legal advice to any individual, district, or other entity.

## ***Part I. Comprehensive Approach***

### ***1. Protection and Empowerment***

*You'll look up and down streets, look 'em over with care.  
About some you will say, "I don't choose to go there."  
With your head full of brains and your shoes full of feet,  
you're too smart to go down any not-so-good streets.*

- Dr. Suess<sup>1</sup>

---

<sup>1</sup> Geisel, T.S., *Oh the Places You'll Go!* 1990. Random House: New York. The author of this Guide read this section in testimony before the COPA Commission and the NRC Committee.

## **Raising Children to Make Safe and Responsible Choices in the "Real World"**

The development of strategies to address issues of concern regarding the use of the Internet by young people must be grounded in knowledge of effective parenting and educational strategies. Parents and educators already know a great deal about helping young people learn to engage in safe and responsible behavior.

When children are too young to comprehend the dangers, to understand the expectations for their behavior, and to independently engage in safe and responsible decision-making, we keep them in safe places and supervise their activities. We keep them in fenced play yards. When we take our children to places that may be less safe, such as a public park, we even more closely supervise their activities. We also use these public excursions as opportunities to teach our children. We teach them about potential dangers, how to recognize dangerous situations, and what actions to take to keep themselves safe. We introduce these lessons with an understanding of the cognitive development and sensitivities of their age.

We also teach children about our positive expectations for their behavior. We teach them about respect for others and actions that are necessary to support the good of the community. And if they engage in unsafe or irresponsible behavior, we intervene with appropriate discipline. We use transgressions as "teachable moments" to review and reinforce the lessons of safe and responsible behavior.

As children grow, we allow them increasing freedom. We do not expect that teenagers will be satisfied remaining in fenced play yards. But we remain engaged. We know that young people who have parents and other influential adults who remain "hands-on," through active involvement, ongoing communication, and supervision, are much less likely to engage in unsafe or irresponsible behavior.

New issues related to potential dangers and expectations for behavior emerge. Issues that would not have been appropriate to address when a child was younger, such as date rape, become important issues to address at this age. We use the same pattern of instruction -- providing information about the issue of concern, how to recognize a situation presenting the concern, and how to effectively respond to the situation.

In sum, helping children and teenagers learn to engage in safe and responsible behavior involves imparting:

- Knowledge about potential dangers or concerns and expectations or standards for responsible behavior.
- Effective decision-making skills that include being able to recognize situations presenting concerns and knowing appropriate or effective responses to such situations.
- Motivation to behave in a safe and responsible manner. Motivation is grounded in values that promote respect for self, others, and the common good.

## **Helping Children Learn to Make Safe and Responsible Choices in Cyberspace**

How do these basic lessons in raising safe and responsible children translate to the Internet? First and foremost, we have to recognize that even though we may be accessing the Internet from the safety of a classroom or family room, the Internet is very much a public place. Allowing young children to have supervised, open access to the Internet (filtered or not) without close supervision would be the equivalent of leaving a child to play unsupervised in New York City's Central Park. Older children need to have the knowledge and skills to make safe and responsible choices in these public places.

### ***Elementary Students***

Students in elementary school are too young to be fully informed about Internet dangers and should not be expected to be able to engage in safe behavior in unsupervised environments. When children are of elementary school age, their use of the Internet should be almost exclusively in "safe Internet spaces" -- environments that provide access to only pre-reviewed, educationally appropriate sites. Their use of electronic communications should likewise be in safe communication environments, such as a classroom e-mail account.

Experienced Internet researchers know the difficulties in finding the quality resources on the Internet and distinguishing such resources from the non-quality resources. Now imagine a 3rd grade student trying to find the quality resources that are at a 3rd grade reading level! Elementary students should simply not be expected to have the necessary skills to be effective researchers on the open Internet. There are simply too many sites that are not appropriate information resources for students at this level of their education. Far too much time would be spent in unproductive searching, and not enough time learning the subject matter under study.

There are a variety of ways to establish these safe Internet spaces. The most common approaches are district or class educational web sites. Some state education systems offer an education web site. The Oregon School Library Information System at <http://www.oslis.k12.or.us/> is an example of such a service. The Education World has an excellent educational web site for students. Subscription services are available from some educational technology companies. There are also technologies that can be used to provide greater security in the establishment of such safe spaces, including proxy servers and the new Internet Content Rating Association system. Clearly, more work in this area is necessary.

If it is necessary for elementary age children to use the open Internet, they should do so only in highly structured environments with close over-the-shoulder supervision.

Since children in elementary school are also using the Internet at home, parents should be provided with information on how to establish safe Internet spaces on their system at home. Parents can be provided with specific information on establishing the school's educational portal as the default portal on their home browser. Parents should also be provided with Internet safety information that is appropriate for elementary age children.

There is one vitally important safety skill that all children should be taught prior to using the Internet, even in safe environments. All children should know that there is "yucky" stuff on the Internet that, through no fault of their own, may appear on the computer screen. Children should

know that if "yucky" material ever appears on their screen, they should immediately turn off the screen (the process to do this may vary depending on the computer system) and tell a teacher or their parent, if at home.

### ***Secondary Students***

When students are in middle school and high school, access should be more open and the focus should shift to instruction on basic safety skills, supervision, monitoring, and responsive discipline. The primary *protection* at this point should be the student's own skills and motivation. One strong motivation for responsible behavior in school should be the significant likelihood that irresponsible behavior will be detected and result in discipline.

But more importantly, the focus must shift to the importance of making choices on the Internet that are in accord with the teenager's emerging sense of personal identity and moral values. This issue is discussed more fully below.

The best time to begin to more fully instruct students about safe and responsible online behavior is the last year of elementary school or early in middle school. At this age, students will be demanding more freedom on the Internet at home. They will also be old enough to understand issues related to the potential dangers or inappropriateness of certain materials and to successfully utilize safety skills.

Schools may want to engineer a gradual opening of the levels of access, rather than providing precocious and curious beginning middle school students with wide open access on their first day of school. For example, middle schools may want to generally limit student access to Internet safe spaces, but allow specific exceptions. Exceptions may be specific classroom activities that require open access or open access upon request in the library, if the student has been unable to find necessary information in the safe Internet space. Schools may also want to require successful completion of an Internet safety and responsible use class prior to allowing such open access.

## **Addressing Issues of Responsible Behavior**

### ***Moral Development***

To address the question of how to help young people use information and communication technologies in a responsible manner, we must consider how young people learn to engage in an responsible, ethical behavior. Furthermore, we must examine how information and communication technologies and the emerging cyber environment may impact their learning and behavior.

The following discussion comes from the introduction to the author's book *Computer Ethics, Etiquette, and Safety*. This book is distributed by The International Society for Technology in Education<sup>2</sup>.

---

<sup>2</sup> URL: <http://www.iste.org>

As young people grow, their emerging cognitive development enables them to gain increasingly accurate perceptions of the world around them. Three principal external influences combine with this emerging cognitive development to affect moral development and behavior. These factors are:

- Recognition that an action has caused harm. When a young person engages in inappropriate action and recognizes that his or her action has caused harm to another, this leads to an empathic response, which leads to feelings of remorse.
- Social disapproval. When a young person engages in inappropriate action and recognizes that others have become aware of and disapprove of this action, this leads to "loss of face" and feelings of shame.
- Punishment by authority. When a young person engages in an inappropriate action and this action is detected by a person with authority over the young person, this leads to punishment imposed by the person in authority, which can lead to feelings of regret, but also can lead to anger at the authority.

These three external influences not only affect behavior in both young people and older people, they also play a major role in a young person's moral development. During adolescence, young people develop a sense of their own personal identity. This personal identity incorporates an internalized personal moral code. In adolescents and adults, our personal moral code functions as an internal influence for ethical and responsible behavior. Behavior is influenced both by the external factors, as well as the internalized moral code.

When we perceive that we have violated our own personal moral code, we feel guilty -- unless we can rationalize our actions in some manner. We are all willing, under certain circumstances to waiver from our personal moral code. We each have an internalized limit about how far we are willing to waiver from the ideal set forth in our personal moral code. This limit protects against unlimited inappropriate activity<sup>3</sup>.

There are a number of factors that appear to influence behavior that waivers from our personal moral code. We are more likely to waiver when our assessment is that:

- There is an extremely limited chance or no chance of detection and punishment.
- The inappropriate action will not cause any perceptible harm.
- The harm may be perceptible, but is small in comparison with the personal benefit we will gain.
- The harm is to a large entity, such as a corporation, and no specific or known person will suffer any loss.

---

<sup>3</sup> Based on theories of Nisan and Bandura. Nisan, M. (1991) Limited acceptable morality. In Kurtines, W. M. & Gewirtz, J. L., *Handbook of Moral Behavior and Development, Vol III*. Bandura, A. (1991). Social cognition theory of moral thought and action. In Kurtines, W. M. & Gewirtz, J. L., *Handbook of Moral Behavior and Development, Vol I*.

- Many people engage in such behavior, even though some may consider the behavior may be considered illegal or unethical.
- The entity or individual that is or could be harmed by the action has engaged in unfair or unjust actions.

### ***Impact of Information and Communication Technologies***

Information and communication technologies have a profound impact on the external influences of behavior.

#### **Technology does not provide tangible feedback.**

When people use technology, there is a lack of tangible feedback about the consequences of actions on others. People are distanced from a perception of the harm that their behavior has caused.

This lack of tangible feedback undermines the empathic response, and thus undermines feelings of remorse. The lack of tangible feedback makes it easier to rationalize an inappropriate action.

#### **Technology allows us to become invisible.**

In fact, people are not totally invisible when they use the Internet. In most cases, they leave "cyberfootprints" wherever they go. But despite this reality, the perception of invisibility persists. Some actions using technology are quite invisible, such as borrowing a friend's software program and installing it on your own computer. It is also possible to increase the level of invisibility with the use of technology tools. Establishing a pseudonymous account enhances invisibility. The fact that many people may be engaged in a similar activity also leads to a perception of invisibility because individual actions are such a "drop in the pond" that they are unlikely to be detected.

Invisibility undermines the potential impact of both authority and social disapproval. If a transgression cannot be detected and a person is unlikely to be punished, threats of punishment are not likely to have any impact whatsoever on behavior.

The issue of the impact of invisibility on human behavior is not new. Plato raised this very same issue in his story about the Ring of Gyges. In this story, a shepherd found a magical ring. When the stone was turned to the inside, the shepherd became invisible. Thus questions were raised: How will we choose to behave if we are invisible? Will we do whatever we want to do because we know that nobody can catch and punish us? Will we do something that could hurt someone because we know that nobody can tell who did this? Or will we do what we know is right?

It is important to recognize that young people are using the Internet, and thus are influenced by the lack of tangible feedback and perceptions of invisibility, at the same time that they are in the process of developing their internalized personal moral code. We do not know how this will affect their development and internalization process.

## ***Strategies to Address Lack of Tangible Feedback and Invisibility***

### **Focus on Personal Values**

*Help young people learn to do what is right in accord with their own personal values, regardless of the potential of detection and punishment.*

To do this, we must enhance their reliance on their own internalized personal moral code. We must shift our focus away from rules and threats of punishments. Threats of punishment are simply an ineffective approach when the likelihood of detection and punishment is so remote. The message: "Don't do this because it is against the rules" has limited impact if you believe that you are invisible and that your actions cannot and will not be detected and punished.

Within the school environment, there clearly should be a lack of invisibility due to the effective supervision and monitoring strategies. But outside of the school environment, the perception and reality of invisibility will exist. Our goal as educators should be to prepare students for this environment.

The key to such preparation is education and appropriate discipline. We must focus the attention of young people on the *reasons* for the rules, rather than the potential of detection and punishment. Rules are generally enacted because actions that violate the rules can cause harm to someone else. So our focus must be on the potential harm, not the rule. In a world where we are invisible, a much more powerful message is: "Don't do this because if you do you will harm someone by (describe the possible harmful impact of the action)." By focusing on the reasons for the rules, we can help young people develop a more understanding and caring moral code.

### **Recognize Unseen Harm**

*Help young people understand how actions can cause harm to people they can not see.*

Empathy actually has two components -- a feeling component and a thinking component. When we see or hear someone who is happy or sad, we begin to feel the same way inside. This is the feeling part of empathy. As young people grow, they also gain the ability to understand cognitively how other people think and feel. They learn to look at things from their perspective. This is the thinking part of empathy. Thinking about how someone else feels can also affect how we feel inside. The lack of tangible feedback impairs the feeling component of empathy. We must help young people learn to rely on the thinking part of empathy when they use information technologies.

### **Use Effective Decision-Making Strategies**

*Help young people learn to use effective decision-making strategies to help guide their behavior in a responsible way.*

These strategies must be effective even though young people do not have tangible feedback and may perceive themselves to be invisible. Effective decision-making strategies, written in language that can be used to communicate with young people include:

- Golden Rule Test *How would you feel if someone did the same thing to you? If you would not*

want to have someone do the same thing to you, then the action is probably wrong.

A version of the Golden Rule is found in every religion in the world. Considering how we would feel if someone did the same thing to us is a powerful ethical decision-making strategy.

- Trusted Adult Test *What would your mom or dad, guardian, or another adult who is important in your life think? Your parents, guardians, or other adults who are important to you may not understand the Internet, but they know a lot about deciding whether an action is right or wrong. Considering how your parents, guardians, or other important adult would judge your actions, you will help you to act in accord with your family's values.*

Philosophers call this the Moral Exemplar. Young people can be encouraged to model the behavior of those whose opinions are important to them. This test also brings in the importance of acting in accord with the values that have been established by the family.

- Is There a Rule? Test *Generally, rules or laws have been created to protect the rights of people and to serve the common good. Rules and laws provide good guidance on whether or not an action is right or wrong.*

It is important for young people to recognize the basis upon which rules have been created. Rules are created to protect the rights of people and to serve the common good. The focus must always be on the reason for the rule, not the rule itself. This is a very important distinction. Young people may think that if they are invisible and no one can punish them for violating a rule, then the rule is of no importance.

- Front Page Test *If your action were reported on the front page of the newspaper, what would other people think? One way to make good decisions is to act as if the whole world can see what you are doing.*

The Front Page Test is another decision-making strategy that can help to address the perceptions of invisibility. There have been a number of widely reported incidents where an individual thought his or her actions were private, only to find them ultimately reported on the front pages of various newspapers.

- If Everybody Did It Test *What would happen if everybody made a decision to do this? Consider what kind of world this would be if everyone did what you are thinking of doing. You might think that you are only causing a "little bit of harm." But if everyone else is also doing a little bit of harm, then someone else might be suffering a lot of hurt.*

This test is an updated version of Kant's Moral Imperative. Encourage students to add up the large amount of harm caused by many people engaging in small acts of harm.

- Real World Test *Would it be OK if you did this action, or a similar action, in the real world? Just because you do something in cyberspace, does not mean that you cannot hurt someone. Actions in cyberspace can cause just as much harm to someone else as actions in the real*

world.

Considering actions in the context of the "real world" can help to create a better understanding of the consequences of actions on unseen others. The Real world Test will help to bring about a better understanding of the real harm caused to real people.

- **Gandhi Test** *Sometimes when people behave inappropriately on the Internet they claim that they are actually trying to make the Internet a better place. Mathama Gandhi was a great leader in India who led a successful revolution using nonviolent resistance. One of the things he said was: "We must the future we wish to see. It is a good thing for people to try to make the Internet and the world a better place. But you will be most successful in making things better if you behave in a way that you want others to behave.*

### **Ensure Accountability**

*Remain "hand's on" while young people are learning these lessons.*

The children of parents who are "hand's on" -- that is know where their children are, what they are doing, and who they are doing it with -- and who keep lines of communication open, are much less likely to engage in risky behavior. When young people are using the Internet, responsible adults in their environment need to remain "hand's on." Effective supervision and monitoring are essential strategies to remain "hand's on."

### **NRC Report Findings and Observations**

On May 8, 2002, the National Research Council (NRC) released its report entitled *Youth, Pornography and the Internet*<sup>4</sup>. A major conclusion of this report was:

(S)ocial and educational strategies to develop in minors an ethic of responsible choice and the skills to effectuate these choices and to cope with exposure are foundational to protecting children from negative effects that may result from exposure to inappropriate material or experiences on the Internet.

The following findings and observations about social and educational strategies contained in the *NRC Report* emphasize the importance of the comprehensive protection and preparation strategies recommended in this Guide:

1. Social and educational strategies directly address the nurturing of character and the development of responsible choice. Because such strategies locate control in the hands of the youth targeted, children may make mistakes as they learn to internalize the object of these lessons. But explaining why certain actions were mistaken will help children learn the lessons that parents and other adults hope they will learn.

---

<sup>4</sup> National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002) URL: [http://bob.nap.edu/html/youth\\_internet/](http://bob.nap.edu/html/youth_internet/).

2. Though education is difficult and time-consuming, many aspects of Internet safety education have been successful in the past several years. While it is true that Internet safety education, acceptable use policies, and even parental guidance and counseling are unlikely to change the desires of many adolescent boys to seek out sexually explicit materials, parents are more aware of some of the other dangers (such as meeting strangers face-to-face) and know more about how to protect their kids better than ever before. (This is true even though more needs to be done in this area.) Children are better educated about how to sense whether the person on the other end of an instant message is "for real." Many of them have developed strategies for coping, and children with such strategies increasingly understand the rules of the game better than their parents. Little of this was true 5 years ago.
3. Social and educational strategies are generally not inexpensive, and they require tending and implementation. Adults must be taught to teach children how to make good choices in this area. They must be willing to engage in sometimes-difficult conversations. And, social and educational strategies do not provide a quick fix with a high degree of immediate protection. Nevertheless they are the only approach through which ethics of responsible behavior can be cultivated and ways of coping with inappropriate material and experiences can be taught.
4. Social and educational strategies have relevance and applicability far beyond the limited question of "protecting kids from porn on the Internet." For example, social and educational strategies are relevant to teaching children to:
  - Think critically about all kinds of media messages, including those associated with hate, racism, senseless violence, and so on;
  - Conduct effective Internet searches for information and navigate with confidence;
  - Evaluate the credibility and motivation of the sources of the messages that they receive;
  - Better recognize dangerous situations on the Internet;
  - Make ethical and responsible choices about internet behavior -- and about non-Internet behavior as well; and
  - Cope better with exposure to upsetting and disturbing experiences and material found on the Internet<sup>5</sup>.

---

<sup>5</sup> NRC, *supra* at Section 10.11.

## ***2. Educational Purpose and Use***

### **Enhancing Student Learning**

The foundation for the development of a comprehensive plan to address the safe and responsible use of the Internet is recognition of the reason for which Internet access is being provided in schools. When a district establishes Internet service, the purpose is not merely to provide students and employees with general purpose, personal access to the Internet. The district system has a very specific purpose: *to enhance student learning and support professional development.*

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

There are several important reasons to be concerned about how students and staff approach the use of the Internet in school.

### ***Tending a Rose***

Two things cannot be on one place. Where you tend a rose, ... a thistle cannot grow.<sup>1</sup>

This passage from the children's book *The Secret Garden* captures an essential reason for the importance on focusing on the educational purpose of the use of the district's Internet system. If the district's technology resources are being used by students who are engaged in exciting, enriching educational activities, there is limited opportunity for students to be engaged in inappropriate activities.

But if the primary use of the district's technology resources is for "Internet Recess," activities that are primarily for popular culture research or entertainment purposes, not only is the district wasting valuable resources, the district has established an environment where inappropriate activity and misuse is much more likely to occur.

Anytime that a school is having problems with "thistles," the first and most important question that must be asked is, "How is the school tending its roses?"

### ***Prevention of the Displacement of Learning***

Educators have precious little time to assist all students in achieving challenging academic standards. The primary use of the Internet should be directly related to achieving learning objectives.

---

<sup>1</sup> Burnett, F. H., (1911) *The Secret Garden*. Harper Collins: New York.

### ***Appropriate Use of Taxpayer Resources***

Taxpayers are supporting the costs of technology in schools because of the promise that technology will assist students in achieving challenging academic standards. Many of the recent articles and reports criticizing increased investments in technology point to the fact that in many schools, technology resources are not being used for their greatest educational purpose.

### ***Preparation for Workplace Use***

The purpose of education is to prepare students for success in life and work in the 21st Century. When students enter the work force, they will likely be using their employer's electronic network that will also be a limited purpose network -- with greater limitations than an education system. Their use on such systems will also be heavily monitored.

An important work skill for students will be the ability to use self-restraint to use a system in accord with its purposes. Companies should not have to rely on Technology Protection Measures to ensure that their employees abide by use restrictions. Schools have a responsibility to help educate young people how to control their usage when they are using a limited purpose system.

### ***Prevention of Problems of Internet Addiction***

There are growing concerns with online addiction -- people who spend hours and hours of time in essentially worthless online activities. When schools force their students to think about their online activities in the context of the value of that activity to their education and self-improvement, schools are assisting students in gaining critically-important self-monitoring skills that will likely assist in preventing addiction.

### ***Personal Account Option***

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

## **Defining an Educational Purpose**

### ***Access to Web***

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

### ***Class- and Instruction-Related***

Activities that are clearly acceptable are class- or instruction-related activities, continuing education, and career development activities for students and professional development and communication activities for employees.

### ***Commercial Use***

Commercial uses should generally be considered unacceptable. This would include the purchasing or offering for sale personal products or services by students.

### **Lobbying**

Most states place a restriction on the use of public resources for lobbying. Therefore, lobbying as defined by state statute would be an unacceptable use. But this limitation should not restrict students from using the system to communicate their opinions to elected representatives. In many states, however, the use of a district system by staff to communicate to elected officials may present concerns.

### **Independent Learning Explorations**

Independent learning explorations may range from serious research to "Internet recess" kinds of activities. One approach a district could take would be to restrict student use to specific class- or instruction-related activities. But this would be equivalent to establishing a school library and then telling students that they can only use the library for class- or instruction-related activities. This approach defeats the purpose of seeking to assist students in learning to use the Internet for their own personal enrichment and learning. It is recommended that high quality, non-entertainment-related, personal research be included in the definition of educational purpose.

### **"Internet Recess"**

What about "Internet recess" kinds of activities. It should be recognized that the vast majority of school libraries contain material related to popular culture, such as sports magazines and books about rock stars or movies, or entertainment materials, such as joke books or books about hobbies. The Internet also contains a vast amount of popular culture materials that have some, but limited, educational value. Innovative teachers may actually be able to make great educational use of such materials. Access to such non-educational or entertainment materials may be considered to be outside of "educational purpose" definition, but schools should allow the use of such materials for teacher-directed instructional purposes. Also many schools establish periods of "open access" where access to such materials is considered to be acceptable.

### **Priorities of Usage**

If a districts or school does allow students to access the Internet for either entertainment purposes or personal research activities, it would be advisable to establish priorities of usage for computers that are available for multiple uses, such as those in the library or an open use computer lab. Students who require access for class- or instruction-related activities should have priority over other uses. A mechanism could be established so that students who are not using the computer for class-related activities could be "bumped" by any student requiring access for a class- or instruction-related purpose.

### **Information Gathering**

As noted in "Transition to a Comprehensive Approach," schools should collect data on the manner in which the technology is being used in the multiple use areas. If schools are finding that an excess amount of the use is for "Internet Recess", this is a clear indication that insufficient attention is being paid professional development and other activities necessary to support the effective use of the Internet for educational purposes activities.

### ***Electronic Communication***

Even sticker questions emerge related to personal electronic communication. Can the principal send an e-mail to her husband asking him to pick up some milk for dinner? Can the science

teacher subscribe to a gardening group discussion? Can a student communicate with a former classmate who recently moved? Can students communicate with each other for personal reasons?

Schools may use different approaches to address issues of electronic communication. One approach is to accept that a small amount of personal communication is to be expected but indicate to all users that overall electronic communication traffic should not be excessive. Any user who engages in excessive traffic that is not to be expected in light of their activities or position may be subject to review of their communication activities. Users should not be allowed to participate in online group discussions, such as mailing lists, unless there is a direct professional development or curriculum-related purpose.

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

## **Strategies to Promote Educational Use**

### ***Professional Development***

*The most essential step necessary to ensure that the district's Internet system is being used effectively to support enriching instructional activities is professional development of the teachers!*

When teachers are prepared to lead students on exciting learning adventures on the Internet, virtually all problems in the use of the Internet disappear. Students become engaged and excited about what they are discovering. The demand for the available computers for completing the assignments will be so high, that "Internet Recess" use will simply not be acceptable. If students do not police themselves, their peers -- who are waiting to get access to complete an assignment - will.

Unfortunately, every assessment of the degree to which schools are reinforcing quality educational use of the Internet and teachers feel prepared to integrate the use of technology into instruction demonstrates that far too many teachers are not yet adequately prepared to use technology and the Internet in an effective educational manner.

Two recent reports include the National School Board Association report *Are We There Yet?*<sup>2</sup> and the Pew Internet and American Life report *The Digital Disconnect: The widening gap between Internet-savvy students and their schools*<sup>3</sup>.

The NSBA survey found that lack of teacher preparation was a significant concern and made the following recommendations:

---

<sup>2</sup> Grunwald Associates (2002) *Are We There Yet?* NSBA Foundation. URL: <http://www.nsf.org/thereyet/index.htm>

<sup>3</sup> Levin, D. & Arafah, S. *The Digital Disconnect: The widening gap between Internet-savvy students and their schools*. Pew Internet and American Life. Report released August 14, 2002. The full report is available online at: URL: <http://www.pewinternet.org/reports/toc.asp?Report=67>.

- Treat technology as an integral tool for instruction and administration — not as an add-on. Technology is not a frill, it's essential to effective instruction and school vitality.
- Use the Internet for core educational priorities that matter most to student achievement. School district leaders report strong interest in online opportunities that match federal, state and local pressures, including standards, assessments and test preparation. School decision-makers should be informed by these priorities as they make choices. At the same time, schools should understand that they can harness the power of the Internet to create and support diverse learning communities.
- Invest significantly in professional development for school leaders and teachers. A broad theme emerging from survey results is that teachers need help incorporating the Internet into regular classroom instruction. For new and veteran teachers alike, the Internet is a new frontier — and one that many have little time or training to explore. Teachers need technology training to be able to use the Internet as an effective, interactive tool for teaching, learning communicating. Teachers also need to be prepared to guide and assess students in different ways.

The need for a focus on professional development was echoed by the Internet savvy teens were surveyed for the *Pew Report*, which noted:

While students relate examples of both engaging and poor instructional uses of the Internet assigned by their teachers, students say that the not-so-engaging uses are the more typical of their assignments. Students repeatedly told us that the quality of their Internet-based assignments was poor and uninspiring. They want to be assigned more—and more engaging—Internet activities that are relevant to their lives. Indeed, many students assert that this would significantly improve their attitude toward school and learning<sup>4</sup>.

The Summary of Findings of the *Pew Report* are set forth in Part V. All readers are encouraged to read the full report, which is available online.

There are many excellent resources for information related to professional development. The International Society for Technology in Education has developed recommended standards for professional development for teachers and administrators<sup>5</sup>, the National Educational technology Standards for Teachers (NET\*T) and the Technology Standards for School Administrators (TSSA, also now called the National Educational Technology Standards for Administrators or NET\*A). These standards provide an excellent overview of the necessary knowledge and skills for all teachers and administrators.

### ***Curriculum Development***

Teachers who are early adopters of technology tend to take great delight in the independent development of innovative lesson plans using the Internet. Unfortunately, these early adopters

---

<sup>4</sup> Levin, supra. Summary of Findings.

<sup>5</sup> URL: <http://cnets.iste.org>.

tend to also be the most actively involved in district or school technology coordination and unfortunately sometimes do not recognize that the vast majority of teachers do not have the time, skills, or inclination to develop their own Internet-based learning activities and curriculum. Second stage adopters also tend to have a basic discomfort because of the probably accurate perception that their students are much more comfortable using the Internet than they are. Second stage adopters do not like to take risks.

To move beyond early stage adoption of the use of the Internet for educational activities requires a shift from approaches that support intuitive early adopters, who like to explore and take risks, to approaches that support more pragmatic second stage teachers, who tend to want to manage any risks that might be present when they and their students step onto the Internet. Second stage adopters can be very effective and successful in their use of the Internet if they have access to lesson plans that have already been developed and tested and to the support of other teachers.

The best way to engage second stage technology adopters is to:

- Provide easy access to risk-free, easy to implement Internet-related lesson plans and activities that are directly related to district curriculum objectives. This can be accomplished through a district, state, or regional web site or through links from the district site to such resources.
- Establish subject and grade oriented mailing lists where teachers can be encouraged to discuss curriculum issues or share lesson plans and where the second stage adopters can rapidly receive support.
- Enlist the aid of first stage adopters to serve as mentors and provide pre-developed Internet curriculum.

### ***Educational Web Site/Portal***

The initial access point for teachers and students should be a district instructional web page that immediately directs students to pre-reviewed, high-quality educational resources.

The U.S. federal government, state departments of education, school districts, public libraries, and companies have been undertaking the responsibility of identifying and reviewing web sites for use in educational settings. Unfortunately, many of these activities are being duplicated, rather than coordinated. Districts can take advantage of many of these existing web development efforts. If the district is providing access to a comprehensive educationally oriented web site that directs students to appropriate resources, there is a much reduced probability that students will be inclined to wander off to other places on the Internet.

### **Educational Purpose and Reliance on Filtering**

The decision to install filtering software may lead to complacency with respect to maintaining a strong focus on educational uses of technology. This may result in the use of taxpayer-supported technology resources primarily for "Internet recess."

In many schools, filtering has become the substitute for professional development and appropriate supervision that are necessary to ensure that tax-payer resources are being used for effective educational purposes. A study published by N2H2, a filtering software company, demonstrates this concern. N2H2 analyzed data relating to student use through their system<sup>6</sup>. The report presents disturbing implications related to the degree to which the Internet is being used in schools for actual instructional related purposes.

N2H2 studied the top 300 sites visited by students by number of page views. According to N2H2, these 300 sites accounted for "roughly half" of the total page views. N2H2 considered their data to present a "representative picture of use." N2H2 indicated that an analysis of data by average per-page viewing time presented the best approach to analyzing how students were using the Internet. N2H2 provided the data in terms of categories and average viewing time (columns #1 and #2). Additional calculations of percentage of viewing time (column #3) were added by the author of this document.

1. Instructional, Reference & Computing	60 seconds	16.7%
2. News & Sports	58 seconds	16.2%
3. Business & Finance	52 seconds	14.5%
4. Commerce & E-Services	51 seconds	14.2%
5. Music, Games & Fun	48 seconds	13.4%
6. Portals & Search	46 seconds	12.8%
7. Communities	44 seconds	12.3%

Here are N2H2's definitions of the categories, followed by analysis and comment:

**Instructional, Reference, & Computing.** Sites that could be use for specific instructional purposes by teachers or students, general research and reference resources, and computer network resources.

One may ask why computer network resource sites were included in this category, since such sites are clearly not instructional purpose sites. If computing sites, which tend to be very popular, were eliminated from this category, this would reduce the percentage of time spent on instructional sites below the already abysmally low 16.7 %.

**News & Sports.** Online versions of national news, sports magazines, local news.

Some of this access may be directly class-related, other access would be considered appropriate within an educational purpose as appropriate independent study.

**Business & Finance.** Financial news sites and online brokerage firms.

Some instructional activities may involve access to business news and finance sites. It is hard to interpret usage in this category. One might query whether N2H2 was also collecting staff usage data.

---

<sup>6</sup> This report is no longer on the N2H2 web site. Please contact for author for more information.

Commerce & E-Services. Commercial sites offering products or online services.

Unless used for a specific educational purpose under the guidance of a teacher, these are "Internet Recess" sites. It can be assumed that most of this access was *not* for instructional related purposes.

Portals & Search. Sites that attempt to branch out and connect users with content.

The amount of time that such portals and search sites were used for instructional related purposes is probably roughly equivalent to the overall use levels.

Music, Games, & Fun. Sites geared towards entertainment and leisure.

Unless used for a specific educational purpose under the guidance of a teacher, these are "Internet Recess" sites. It can be assumed that most of this access was *not* for instructional related purposes.

Communities. Sites providing content targeted to specific demographic groups and typically containing a large amount of user generated content such as chat and message boards.

It is also likely that much of this activity was *not* for instructional related purposes.

N2H2 was only able to classify the data by its descriptive criteria. N2H2 had no data on how such sites were actually being used. It is true that innovative teachers can make effective use of entertainment or commerce sites for instructional activities, but based on anecdotal reports of how the Internet is being used in many schools that have not places a strong focus on professional development, it is not likely that much of all of the reported use in the non-educational categories was for teacher-directed, educational activities.

What we can reasonably conclude, based on this limited data, is less than 16.7% of student use was on sites that were clearly instructional related. It is also highly probably that a good portion of the 54.4 % of student use in the Business and Finance, Commerce and E-services, Music, Fun & Games, and Communities categories was not for instructional related purposes, rather were "Internet Recess" activities.

Unfortunately, as there are no research funds available to investigate these issues further, this assessment and analysis cannot be considered definitive. It is unknown what the usage patterns are in schools without filtering. But at the very least, it is not accurate to conclude that the use of filtering software is reinforcing effective *educational use* of the Internet.

### ***3. Education about Safe and Responsible Use of the Internet***

#### **International Society for Technology in Education Technology Education Standards**

The recommendations for student instruction and professional development for administrators and teachers contained in this Guide are in accord with the technology education standards developed by the International Society for Technology in Education (ISTE), in partnership with other educational organizations<sup>1</sup>.

The pertinent standards are as follows:

#### ***National Educational Technology Standards for Administrators (NET\*A)***<sup>2</sup>

VI. Social, Legal, and Ethical Issues – Educational leaders understand the social, legal, and ethical issues related to technology and model responsible decision-making related to these issues. Educational leaders:

- A. ensure equity of access to technology resources that enable and empower all learners and educators.
- B. identify, communicate, model, and enforce positive social, legal, and ethical practices to promote responsible use of technology.
- C. promote and enforce security and online safety related to the use of technology.
- D. promote and enforce environmentally safe and healthy practices in the use of technology.
- E. participate in the development of policies that clearly assign ownership of intellectual property developed with district resources.

#### ***National Education Technology Standards for Teachers (NET\*T)***<sup>3</sup>

VI. SOCIAL, ETHICAL, LEGAL, AND HUMAN ISSUES. Teachers understand the social, ethical, legal, and human issues surrounding the use of technology in PK-12 schools and apply those principles in practice. Teachers:

- A. model and teach legal and ethical practice related to technology use.
- B. apply technology resources to enable and empower learners with diverse backgrounds, characteristics, and abilities.

---

<sup>1</sup> URL: <http://cnets.iste.org>.

<sup>2</sup> URL: <http://cnets.iste.org/tssa/>. Originally referred to as Technology Standards for School Administrators.

<sup>3</sup> URL: <http://cnets.iste.org/index3.html>.

- C. identify and use technology resources that affirm diversity
- D. promote safe and healthy use of technology resources.
- E. facilitate equitable access to technology resources for all students.

***National Education Technology Standards for Students (NET\*S)<sup>4</sup>***

2. Social, ethical, and human issues

- Students understand the ethical, cultural, and societal issues related to technology.
- Students practice responsible use of technology systems, information, and software.
- Students develop positive attitudes toward technology uses that support lifelong learning, collaboration, personal pursuits, and productivity.

## **Instruction for Staff**

### ***Administrator Instruction -- A Priority!***

As was reported in the *Digital Disconnect*, the Pew Internet and American Life survey of Internet savvy teens, the role of administrators in the use of technology in schools is of critical importance.

School administrators—and not teachers—set the tone for Internet use at school. The differences among the schools attended by our students were striking<sup>5</sup>.

Internet savvy teens have picked up on what educational technology professionals have also come to recognize: The knowledge, understanding, and support for the effective use of technology for instructional purposes demonstrated by school administrators is what sets the tone for the use of the Internet at school.

Unfortunately, while much emphasis has been placed on professional development for teachers in the use of technology, there has been far too little focus on professional development for administrators.

Administrators simply cannot provide the leadership that is necessary and critical to the establishment of a school environment that supports the safe and responsible use of the Internet by students and staff if they do not understand the critical issues that underlie the foundation of such an environment.

---

<sup>4</sup> URL: <http://cnets.iste.org/index2.html>

Levin, D. & Arafah, S. *The Digital Disconnect: The widening gap between Internet-savvy students and their schools*. Pew Internet and American Life. Report released August 14, 2002. The full report is available online at: URL: <http://www.pewinternet.org/reports/toc.asp?Report=67> Summary of Findings.

The lack of understanding by administrators of these issues can also have significant financial repercussions for the district. As discussed in "District Liability to Students and Other Liability Issues" and "Student Speech," some school districts have suffered financial loss as a result of inappropriate disciplinary responses implemented by the building principal.

### ***Teachers and Other Staff***

Teachers and other staff, especially those with responsibilities related to monitoring of student use of the Internet, also need to have a good grounding in issues related to the safe and responsible use of the Internet. All staff should understand that their use of the Internet through the district system must be in compliance with the Internet Use Policy and that their use is also monitored. Far too often, when instances of misuse are identified, the offender is a school staff person, ranging from the relief custodian to the superintendent.

Teachers need to be especially knowledgeable about activities that they may undertake that could be in violation of the policy -- such as directing all of their students to sign up on a "cool new commercial site" they have discovered. These sites that may be collecting personal information and market research data on their students.

Teachers also need to understand and be attentive to indicators that may provide clues that a student may be engaging in highly inappropriate or potentially dangerous online behavior. Teachers also need to be attentive to student use that may be harassing or bullying other students.

An important aspect of instruction regarding the safe and responsible use of the Internet relates to the effective use of those "teachable moments" that will naturally occur in the context of all Internet use. For example, a well-prepared teacher can use an instance of a student's incorporation of a copyrighted material into a multimedia project as the opportunity for a discussion about how the principles of copyright law apply to such use.

### ***Substitute and Student Teachers***

A district's well-developed approach to the safe and responsible use of the Internet can be undermined by the failure of substitute teachers or student teachers to understand the basic principles of the district approach and their responsibilities when engaging students in Internet-related educational activities.

It is recommended that substitute teachers must be specifically approved to instruct in classrooms where students are accessing the Internet. Approval requirements will ensure that substitute teachers have a standard level of technical proficiency and understand Internet safety and responsible use issues, this policy, and the obligations related to supervision of students in their use of the Internet.

Student teachers should receive the same instruction prior to being allowed to provide instruction to students involving the Internet, outside of the supervision of their cooperating teacher.

Districts may want to consider the establishment of periodic training sessions so that substitute teachers and student teachers can learn about the district's comprehensive approach, the district's Internet Use Policy, and their responsibilities when directing student use of the Internet.

## **Instruction for Parents**

Schools should be encouraged to undertake the important responsibility of providing parents with education around issues of the safe and responsible use of the Internet by young people. If parents have greater understanding of the critical issues, this will likely contribute to their support for the comprehensive approach taken by the district.

Unfortunately, far too many parent education programs around safety on the Internet have focused on "how to choose and install filtering software." Parents are simply not choosing this approach. As noted in the *NRC Report*,

A survey conducted by Family PC magazine in August 2001 found that of 600 families surveyed, 26% used parental controls of some kind. About 7 percent of those using parental controls (about 1.8 percent of the total) used off-the-shelf store-bought filtering software. The rest used filtering offered by an Internet service provider<sup>6</sup>.

The single most important concept to address with parents is the critical importance of remaining involved in their child's activities related to the Internet and not overreacting if their child reports to them or if they find that their child has inadvertently or intentionally gotten into the Information superhighway gutter.

In a survey taken by the Kaiser Family Foundation and National Public Radio in 2001, it was noted that about three-fourths of the parents said that they had rules related to the use of the Internet, but only half of their children reported the existence of such rules. Only 38% of older children, those aged 14 - 17, said that their parents knew "alot" about the things they do on the Internet and the Web sites they visit.

Of greatest concern is a finding in a study of girls' use of the Internet conducted by the Girl Scouts.

Girls are aware of the varied dangers of the Internet, but want more proactive involvement rather than prohibitive don'ts from parents. All too often, these computer-savvy teenage girls are still naive and emotionally vulnerable, and they report grappling with issues such as how to react to sexual online content they unwittingly encounter.

A startling example: 30 percent of girls responding to the study reported that they had been sexually harassed in a chat room, but only 7 percent told their mothers or fathers about the harassment, most fearing their parents would overreact and ban computer usage altogether<sup>7</sup>.

---

National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002). URL: [http://bob.nap.edu/html/youth\\_internet/](http://bob.nap.edu/html/youth_internet/) at Section 12.1.1, footnote 10.

<sup>7</sup> Whitney, R. (2002) *The Net Effect: Girls and New Media*. Girl Scout Research Institute, New York. URL: <http://www.girlscouts.org/about/PDFs/NetEffects.pdf>

Parents simply *must recognize* that if their children fear that their reaction to a report of problems encountered on the Internet will be to get angry, blame the child, and restrict Internet access, children are simply *not* going to make such reports. As a result, children will essentially be on their own when facing the dark side of the Internet.

Schools are the institutions in our society that have the most direct relationship with parents. Schools should undertake the important responsibility of providing parent education related to use of the Internet.

## **Instruction for Students**

### ***Outline of Safe and Responsible Use Issues***

The following is a recommended outline of issues to address related to the safe and responsible use of the Internet. An overarching instructional focus should be on media and information literacy, which will provide an important foundation for the following topics.

- Avoiding unintentional access – effective search skills, URL porn-napping.
- Dealing with accidental access – getting out of mouse-traps, reporting.
- Recognizing and dealing with unwanted SPAM.
- Communication safety skills – protection of privacy, recognizing predators, reporting predators, protecting friends.
- Protection of privacy – personal privacy, privacy of others, privacy on commercial sites, profiling.
- Harmful speech – defamation, harassment, violation of privacy, abusive language, flame wars, etiquette, recognizing harmful speech/hate sites, consequences for offenders, effective victim responses.
- Responsible speech – free speech rights, effective online advocacy, disability IT access.
- Copyright – rights and responsibilities.
- Plagiarism.
- Computer security – unlawful computer activities.
- Network security and resource limits – passwords, viruses, quotas, downloads, group lists.
- Online addiction – sexual, violent games, gambling, other.

Please consider the book, *Computer Ethics, Etiquette, and Safety for the 21st Century Student*, by Nancy Willard, published by the International Society for Technology in Education<sup>8</sup>. Additional resources for professional development and parent education are under development by the Responsible Netizen Institute.

### ***Internet Use Policy as the Foundation***

As noted in the chapter entitled "Internet Use Policy," the policy provisions can be considered the foundation for an instructional program for administrators, staff, and students, related to the safe and responsible use of the Internet. A district objective should be that all administrators, staff, and secondary students know the provisions of the Internet Use Policy and regulations and, more importantly, understand the underlying reasons for the policy and regulation language.

### ***Transition at Middle School***

For students, the time that instruction about the Internet Use Policy will be most important is in preparation for use of the Internet in middle school. This is the time when students are generally granted more freedom of the use of the Internet at school. This is also the time when they are most likely expanding their use of the Internet at home.

Establishing a specific instructional program where students will engage in an in-depth analysis of the district's Internet Use Policy and the reasons for the provisions should occur in conjunction with the transition to middle school. Such instruction might occur during the last half of the year in elementary school or as an entry course in middle school.

As a result of successful completion of this course, students could obtain some form of certification, an Internet "driver's license," that would enable them to have the privilege of more open use of the Internet. It will be necessary to establish some manner of providing for instruction of those students who transfer into the district at a later time.

Care will need to be taken to help students understand what provisions of the policy are related specifically to activities that are not considered to be appropriate in school and what provisions set forth good guidelines for safe and responsible use in any location.

### ***Elementary School***

Students in elementary school are presumably using the Internet in safe Internet spaces while at school. Students in these grades, and their parents, still should receive instruction in essentially Internet safety skills, especially those related to avoiding the inadvertent access of inappropriate sites and skills for independently dealing with the potential of accessing such sites. These essential skills are addressed below.

### ***Incorporation into the Curriculum***

Issues related to the safe and responsible use of the Internet should be incorporated, where appropriate, into specific areas of the curriculum. Logical courses that should be adapted to incorporate Internet use issues include:

---

<sup>8</sup> Available through ISTE's online bookstore at URL: <http://www.iste.org>

- Sex education classes – Internet pornography, predation and victimization, online addiction.
- History and social science – online hate/harmful speech, free speech/responsible speech, digital divide, effective online advocacy.
- Writing instruction – copyright and plagiarism.
- Technology classes – copyright, technology ethics, computer security.
- Web development projects – copyright, plagiarism, harmful speech, free speech, privacy, disability IT access.
- Consumer education – online profiling and marketing, Internet scams and frauds

Media and information literacy should be addressed throughout curriculum.

## ***4. Internet Use Policy***

### **Issues to Address Related to Internet Use Policies**

#### ***Components***

The Part IV this Guide sets forth a Checklist for the Development of a Comprehensive Safe and Responsible Internet Use Plan that districts or schools can use to assess the degree to which they have addressed the issues raised in this Guide. Additionally, Part IV includes recommended policy and regulation language for a District Internet Use Policy and Regulations.

Many people call the policy related to Internet use an "Acceptable Use Policy" or AUP". The term used in this Guide is Internet Use Policy because of the perspective that such policies must address more issues than simply what is acceptable or unacceptable. Basically, the terms can be used interchangeably.

#### ***CIPA***

As addressed in "Compliance with the Children's Internet Protection Act" the provisions set forth in CIPA for inclusion in an Internet Safety Plan provide an excellent framework for the development of a District Internet Use Policy. The chapters in Part II of the book follow the CIPA requirements as a framework.

#### ***Readability***

The average student in 5th grade should be able to read and understand the district policy, if guidance is provided by a teacher for some of the concepts. Far too many policies are written at a language level that is too complex -- for both students and teachers.

#### ***Clarity***

Restrictions on student activities should be written with sufficient clarity to allow the students and staff to have a good idea of where the boundaries between appropriate and inappropriate lie. Students need to know this information so that they can manage their own behavior. Staff need to understand the expectations so that they do not inappropriately discipline a student for engaging in activities that are appropriate under the policy, but inappropriate under their own value system. The incident related in "District Liability to Students and Other Liability Concerns" involving a lab monitor and a principal who told a student that she could not look at a site with non-traditional religious information provides an illustrative point.

Obviously, with respect to access to inappropriate material, there will always be some differences of opinion regarding the degree to which certain material should be considered appropriate or inappropriate. Secondary staff should receive instruction regarding the policy addressing the boundaries of appropriate and inappropriate with respect to Internet material.

#### ***Communication***

The *NRC Report* noted:

Furthermore AUPs must be read, and young people must take them seriously. In a number of site visits, students appeared to be relatively ignorant of what their school's AUP stated. A number of teachers noted that they believed AUPs were not generally read, because they were simply one of a large number of forms that students had to bring back signed. ... Thus some explicit attention in the school ... to the AUP is warranted to underscore its importance<sup>1</sup>.

The Internet Use Policy should be more than a form that is sent home to be signed by a parent. The "more" is addressed in the next section.

## **Internet Use Policy as Foundation for Instruction**

The Internet Use Policy should be viewed as providing the foundation for the instruction that students and staff will receive regarding the safe and responsible use of the Internet. The Internet Use Policy will provide the "rules." It is exceptionally important that students and staff understand the "reasons" for the "rules." If students and staff are unable to understand the rules in the context of the concerns and issues the rules are meant to address, the policy will have limited value as a tool to promote the safe and responsible use of the Internet.

The most important time to have a serious discussion with students about the provisions in the district's Internet Use Policy will be either near the end of 5th grade, as students are preparing for their new educational environment, the middle school. Alternatively, such instruction can be addressed in a special program for students entering middle school. This is the point at which the focus will shift from protection, to preparation and accountability. By coincidence, 5th grade is also the time that most students are first exposed to "sex education." It would seem logical to include in the sex education presentation a discussion about quality sexual education information and other not-so-healthy sexual material that is present on the Internet.

## **Creation and Implementation**

### ***Creation***

As discussed in "Transition to a Comprehensive Approach," it is envisioned that the creation, modification, and periodic evaluation of the District Internet Use Policy would be the responsibility of a district-level committee with representatives of all stakeholders. The process for development or modification should include the provision of information to the various stakeholder groups, with the opportunity provided for input and feedback.

### ***Policy or Regulations***

Some districts prefer to have all provisions related to student and staff Internet use included in a policy that is reviewed and adopted by the board. If there is a need for a minor change, this can present concerns related to the process necessary for accomplishing such change.

The approach taken in the Policy and Regulation materials set forth in Part IV of this book is that of setting forth a relatively brief board policy that outlines the overall objectives and delineates

---

<sup>1</sup> National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002). URL: [http://bob.nap.edu/html/youth\\_internet/](http://bob.nap.edu/html/youth_internet/), at Section 10.6.

responsibilities. This Policy should contain provisions that are necessary for districts to be in accord with CIPA. Then the Regulations contain the implementation details. These Regulations can be more easily modified by staff in the event of a necessary, but minor, change. Additional detail could be addressed in some form of attachments made to or guidelines that may accompany the Regulations.

An additional form is the Student Use Agreement, which contains only those provisions of the policy that address student use issues.

### *Signatures*

Most districts go through a process of having students and parents sign the Internet Use Policy. This process is slightly different than the process used to address other student discipline issues. Most districts do not require students and parents to sign their willingness to abide by the district's other disciplinary rules. Some districts are transitioning to an approach that provides the policy with the ability for parents to have their child "opt out" of having Internet access.

However, there are four reasons why it is advisable to obtain a parental signature on an Internet Use Agreement. These reasons are:

- Limitation of liability. The best way to prevent problems related to parental overreaction to issues of concern related to Internet use, that could lead to litigation is through the use of a warning of the possible dangers on the internet, a disclaimer of liability, and the option for parents to not allow their child to use the Internet. If an upset parent goes to visit an attorney and the attorney obtains a copy of the Internet use agreement, the parental signature on this form will likely stop an such proposed litigation. These issues are more fully discussed in "District Liability Related to Access to Inappropriate Material or People."
- Permission for disclosure of student information on the Internet. Prior to disclosing student information on the Internet, the district must have parental permission. Since such permission is absolutely necessary, it makes sense to include the provisions requesting permission for such disclosure in a full Internet Use Agreement. These issues are more fully addressed in "Disclosure of Student Personal Information."
- Copyright permission. Prior to posting student work on the Internet, it is recommended that the district receive permission (in copyright terminology this is called a "license") to post such work.
- Parental education. The district's Internet Use Policy can provide a form of education to parents about important safe and responsible Internet use issues. Ideally, the Internet Use Policy can be accompanied by recommendations and guidance from the district on addressing Internet use issues at home<sup>2</sup>.

There is no reason why the process of having a parent and student sign the Internet Use Policy should be required to be an annual event. The above objectives can be met by having a parent and student sign the document upon enrollment at a particular school. This would shift the

---

<sup>2</sup> Such material is under development at the Responsible Netizen Institute.

document from an enclosure in the annual set of forms, to the packet of papers signed upon enrollment.

Instructions and reminders about the provisions of the policy should be provided periodically throughout the year to the students.

### ***Students Whose Parents Refuse***

As the use of the Internet becomes more of an integral component of the educational experience for students, the refusal by a parent to allow their child to participate will create concerns. In some cases, students simply will not be able to participate in the specific instructional activities. It may be possible for the teacher to arrange for all of the Internet-related materials to be downloaded for the student to access on a computer that does not have live Internet access. The ability and inclination of teachers to do this may vary.

The better job the district can do in providing parent education, the more likely it is that the parent's perceptions of the dangers and risks will be addressed. This is the only long-term solution to this particular issue.

## ***5. Supervision, Monitoring, and Appropriate Discipline***

### **CIPA Requirements**

The CIPA requirements for an Internet Safety Plan include a requirement of monitoring. Chapter 6 in Part II repeats some of the following information.

### **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<sup>1</sup>

### ***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.

---

<sup>1</sup> National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002). URL: [http://bob.nap.edu/html/youth\\_internet/](http://bob.nap.edu/html/youth_internet/), at Section 12.2.5.

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 supervising 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.

### ***Appropriate Discipline***

Misuse of the Internet by students should be addressed in a manner that makes use of the "teachable moment" both for the individual student and other students in the school. The focus of such instruction should be on the reasons for the rule -- the issues or concerns regarding potential harm that the rule is designed to address -- rather than a focus on disobedience or the power of the teacher or administrator to impose discipline.

As discussed in Chapter 1, the Internet poses significant issues related to moral development and ethical decision-making. Use of the technology leads the user to perceive that he or she is invisible. The reason for effective supervision and monitoring in school is to address the invisibility concern.

But students will also be using the Internet in locations outside of school. Just as educators seek to prepare students to make responsible choices in other areas of their lives, educators should seek to assist students in learning to make responsible choices when they use the Internet and other information and communication technologies. This requires a shift from a authoritarian, punitive response to consequential response.

The lack of tangible feedback, which distances the student from being sensitive to the harm caused by his or her misuse, can interfere with responsible decision-making. An effective disciplinary response is a response that forces the student to recognize the harm or potential harm that his or her action caused or could have caused. This harm or potential harm provides the reason for the rule. To focus the student's attention on the harm or potential harm requires that

the disciplinary response provide a logical consequence to the specific misuse. If the misuse has involved harm inflicted upon another, the logical consequence is some action that seeks to rectify that harm or acknowledge remorse.

Authoritarian disciplinary responses that merely demonstrate the power of the educational authority to impose discipline – such as merely suspending the student – will not effectively teach the student why his or her actions caused harm. Instead of leading to remorse, such authoritarian responses shift the student’s focus from the harm caused by his or her actions to anger at the authority. While the student may learn not to engage in misuse when there is effective supervision and monitoring that could detect such misuse, such lessons will have no relevance for the many times that the student will be using the Internet under conditions where there is no effective supervision or monitoring.

No student should ever be disciplined for incidents that have occurred that are outside of the control of the student, such as the unintentional access of inappropriate material. No student should ever be disciplined for reporting that they have gotten into a dangerous or concerning online situation.

## **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 been 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<sup>2</sup>. The first part of the test requires "[t]he person must have had an actual or subjective expectation of privacy."<sup>3</sup> The second part requires that this subjective "expectation be one that society is prepared to recognize as 'reasonable.'<sup>4</sup>" 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

---

<sup>2</sup> *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)

<sup>3</sup> *Id.* at 350-52, 360.

<sup>4</sup> *Id.* at 361 (Harlan, J., concurring).

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.*<sup>5</sup>. These standards are:

- Was the search "justified in its inception"<sup>6</sup>? A search is justified when there are "reasonable grounds for suspecting that the search would turn up evidence that the student has violated or is violating either the law or rules of the school"<sup>7</sup>.
- Was the search "reasonably related in scope to the circumstances which justified the interference in the first place"<sup>8</sup>? 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"<sup>9</sup>.

The extent of a district's ability to investigate the personal files of staff is less clear. In *O'Connor v. Ortega*<sup>10</sup>, 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***

#### **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?

---

<sup>5</sup> 469 U.S. 325 (1985).

<sup>6</sup> *Id.* at 341.

<sup>7</sup> *Id.* at 342 (citations omitted).

<sup>8</sup> *Id.* at 342.

<sup>9</sup> *Id.* at 342 (citations omitted).

<sup>10</sup> 480 U.S. 709 (1987).

- 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 than 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 student 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 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.

## ***6. Planning and Implementing a Comprehensive Approach***

### ***Safe and Responsible Internet Use Planning Committee***

Most districts and many schools, have established a technology committee. These committees are the most appropriate committees to also address issues related to the safe and responsible use of the Internet. It is essential that these committees be well-integrated with other key district committees and departments, especially including administration, curriculum, instruction, and library/media. Technology committees should include representatives from all of the major stakeholder groups, including teachers, administrators, technical services, media specialists, secondary students, and parents.

### ***Planning and Policies***

Part IV contains a "District Checklist for the Development of a Comprehensive Safe and Responsible Internet Use Plan." This Checklist presents items that should be considered in the development of a comprehensive education and supervision approach.

Modifications to district policies will need to be approved by the district's governing board. Regulations and operational guidelines can be approved in accord with the district process. Since policies and regulations can be extensive and difficult for many to read, informational material may also be developed for dissemination to parents and the community. Part IV contains documents with recommended language for policies, regulations, and informational materials. All of these documents can be downloaded from this site, modified to meet district or school requirements, and distributed.

The materials have been developed to provide for a relatively brief board policy, which contains all necessary elements for compliance with CIPA. The implementation detail is contained in district regulations, which are more easily modifiable by district educators, without the requirement of board consideration. All of these materials may be adapted as necessary to meet the specific operating procedures of individual districts.

## *Public Disclosure and Information Gathering*

### **CIPA Requirements and FCC Statements Related to Public Disclosure and Information Gathering**

CIPA requires the a public notice and a public hearing in the context of the adoption of the Internet Safety Plan:

PUBLIC NOTICE; HEARING.-- An elementary or secondary school described in clause (i) or the school board, local educational agency, or other authority with responsibility for administration of the school, shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy. ...<sup>1</sup>"

Most districts have already met the CIPA requirements of holding a public hearing. However, it is recommended that the district establish a mechanism to provide for ongoing public input and feedback.

In the development of the Regulations for the implementation of CIPA, the FCC requested the submission of public comment. Several commenters sought to persuade the FCC to implement more extensive public disclosure and information gathering requirements than were contained in the law. The FCC declined to implement the recommendations because they were not required under the terms of the law.

Despite the FCC's determination to reject the recommendations made by some of the commentors, the recommendations make good sense for a school district that is seeking to effectively engage the community and to ensure that their approach to addressing the concerns is accountable. Many of the recommendations have merit from the perspective of enhancing effective planning and community relations.

The discussion of these public disclosure and information gathering requirements by the FCC was as follows:

40. After careful review, we decline to require schools and libraries to publicly post the key requirements of CIPA, the text of the written Internet safety policy adopted, the name of the vendor of the technology protection measure chosen, and instructions on registering complaints. We disagree with commenters that suggest that recipients be required to post this material in a public area, preferably near the Internet computers, and on websites when possible. Commenters argue that this mandated disclosure would inform library patrons and parents of school children about the measures taken to protect against illegal or objectionable content, and would assure that the public would assist in monitoring compliance.
41. The plain language of the statute does not require such disclosures. Congress has not specified what information schools and libraries must disseminate to their relevant communities regarding CIPA implementation choices, and the manner in

---

<sup>1</sup> [47 U.S.C. 254 (h)(5)(A)(i)(III)(iii)]

which they must do so. Because the statute does not require these disclosures, we decline to impose additional burdens on schools and libraries<sup>2</sup>."

42. A few commenters propose mandating that all schools and libraries compile and report specific information about the workings of technology protection measures. Under these proposals, entities would be required, for example, to catalogue (in various categories) the number of attempts made to access prohibited visual depictions, the number of times the technology measure succeeded or failed, and the number of instances where "clearly or arguably appropriate and protected material" was inadvertently blocked or restricted. It has also been proposed that we require all recipients to collect any complaints filed by the public, and make these available. Other commenters oppose these various requirements as not mandated by CIPA, overly burdensome to schools and libraries, and potentially violative of statutory privacy rights of students. Because we concur that these data collection and reporting requirements fall outside the requirements of CIPA, we decline to impose such requirements on recipients. As we have stated previously, we are confident that local authorities will take the appropriate steps to ensure that they have complied with CIPA's requirements<sup>3</sup>.

### **Public Disclosure**

Appropriate public disclosures about the district's efforts to protect and prepare students to use the Internet in a safe and responsible manner can help alleviate parental and community concerns about use of technology and the Internet. Such disclosures can also help parents understand the need to develop comprehensive strategies to reinforce the safe and responsible use of technology by their children at home. Disclosures can help to mitigate problems by communicating information about the district's good faith efforts, as well as providing honest information about the presence of inappropriate material on the Internet. Districts can also use these disclosures as an opportunity to request further input from the various stakeholders that can be used in evaluating and updating the District's Safe and Responsible Internet Use Plan.

Districts may wish to consider the following disclosures and input mechanisms:

- Posting of the District's Safe and Responsible Internet Use Plan on the district web site, with links to the policy and regulations, and an e-mail input mechanism requesting comments or concerns.
- Provision of a brief description of the District's Safe and Responsible Internet Use Plan to parents, in addition to the Student Safe and Responsible Internet Use Agreement and parental permission form.

### **Information Gathering and Analysis**

---

<sup>2</sup> Federal Communications Commission, *In the Matter of Federal-State Joint Board on Universal Service Children's Internet Protection Act. Report and Order*. April 5, 2001. URL:

[http://www.fcc.gov/Bureaus/Common\\_Carrier/Orders/2001/fcc01120.doc](http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc).

<sup>3</sup> FCC Order, *supra*.

The establishment of a regular process for gathering data and evaluating the effectiveness of the District's Safe and Responsible Internet Use Plan is essential for effective ongoing planning. Technologies are changing rapidly, new concerns will inevitably emerge, and the effectiveness of existing strategies must always be assessed.

The District's Safe and Responsible Internet Use Committee should evaluate the following kinds of data and information on an ongoing basis:

- Data related to student Internet use to assess the degree to which the district's Internet system is being used for quality educational activities. E.g. A periodic analysis of a randomly selected subset of 200 - 400 sites accessed by students during the time when they should be using the Internet for educational activities to determine the number of sites that appear to be educationally relevant, as compared to sites that do not appear to be educationally relevant, would provide significant insight into the degree to which the district's investment in technology is being used for quality educational purposes.
- Reported incidents where students have accidentally accessed inappropriate materials. These reports should be analyzed with respect to determining the content and effectiveness of district instruction in avoiding such accidental access.
- Reported incidents of student or staff violations of the District Internet Use Policy. These reports should be analyzed with respect to determining the patterns of behavior that may need to be addressed through better instruction, supervision, and/or discipline.
- Recommendations or input made to the committee from administrators, teachers, parents, students, and community members.