

Choosing Not To Go Down the Not-so-good Cyberstreets

National Academy of Sciences
Committee on the Study of Tools and Strategies for Protecting Kids from
Pornography and Their Applicability to Other Inappropriate Internet Content
Workshop on Non-Technical Strategies to Protect Youth from Inappropriate Material on the Internet
December 13,2000
Washington D.C.

Background Paper provided by
Nancy Willard, M.S., J.D.
Director, Responsible Netizen
Center for Advanced Technology in Education
University of Oregon College of Education
Eugene, Oregon 97403
Web site: <http://netizen.uoregon.edu>
E-mail: nwillard@oregon.uoregon.edu
(541) 346-2895

"When we fall into the trap of believing or, more accurately, hoping that technology will solve all of our problems, we are actually abdicating the high touch of personal responsibility. *** In our minds at least, technology is always on the verge of liberating us from personal discipline and responsibility. Only it never does and never will. The more technology around us, the more the need for human touch.'"

Regardless of issues related to the use, effectiveness, and appropriateness of technology tools, laws, and labeling systems, the simple and plain truth is that virtually every young person in this country will, at one time or another, have unsupervised access to the Internet through an unfiltered and unmonitored system. Any young person who desires to access the "'darkside²" of the Internet will be able to find a way to do so. Technology tools, laws, and labeling systems are insufficient means to prevent such access.

The more important question, therefore, is how can we help young people gain the knowledge, decision-making skills, and motivation to make safe and responsible choices when they are using the Internet.

¹ Naisbitt, J., *Megatrends: Ten new directions transforming our lives*, New York, N.Y. Warner Books, 1984.

² I have chosen to use the term "darkside" to describe the kinds of sites that others are calling "harmful to minors." I believe that we need to tell young people that the reason these sites are "harmful" is that they reflect the "darkside" of humanity. Here is how I have described such sites in a student handbook addressing the safe and responsible use of the Internet: "These sites contain pornography and other profane and obscene materials, hate material and violent games, and information about dangerous or unhealthy activities. The material on "darkside" sites reflects a negative side of human nature. These sites promote violence and hatred. They foster sexual and racial harassment and disregard for the rights of others. They encourage crude attitudes. The individuals creating these sites simply do not share a vision of the world as a peaceful place, where all people and other living things are treated with caring and respect."

What are the issues of concern?

We must address the issue of young people accessing materials that promote violence and abuse -- sexual, racial, animal, or other abuse. As was recently reported, "After reviewing 30 years of research, top members of the public health community have concluded that viewing violent entertainment can lead to increases in aggressive attitudes, values and behavior, particularly in children."³ Clearly, young people's interaction with violent and abusive materials found on the Internet can be predicted to have a damaging effect on values and behavior. Too often, however, the concern is expressed as an issue of how to keep young people safe, when, in fact, young people are intentionally accessing these sites -- an issue of personal responsibility on the part of the young person. We need a greater understanding of what conditions predispose young people to be attracted to these sites and how these sites exploit this predisposition.

We must also empower young people to handle a wide range of interactions and activities on the Internet that could be harmful to their well being. These safety concerns include sexual predation, hate group recruitment, invasion of personal privacy, Internet addiction, Internet fraud and scams, harassment, stalking, and harmful speech, as well as the inadvertent access of harmful material. We cannot expect that reliance on technology "tools" will be effective in addressing these safety concerns. We also cannot expect that young people will always have an adult at their side who is able to recognize and assist in handling these concerns. We must empower young people to recognize the danger signs and handle the situations when they arise. Handling the situation may require calling upon an appropriate adult for assistance or it may require simply dealing with the situation on their own.

We also must address other issues related to the responsible use of the Internet by young people. These issues include copyright infringement, plagiarism, computer security violations (hacking), violation of privacy, Internet fraud and scams, harassment, stalking, and dissemination of violent and abusive material.

Every parent knows how to teach a child to cross a busy street. When children are too young to recognize the danger and do not have the skills to safely negotiate crossing a street, we keep them in safe places and only allow them to approach a busy street when there is an adult present holding their hand. We talk to them about the dangers and teach them the skills necessary to avoid danger. We emphasize the value of making safe choices. Gradually, we allow them more freedom, but are on the watch for any unsafe behavior. If unsafe behavior occurs we use this as a teachable moment to reiterate the dangers and the skills necessary to avoid the dangers. When children are old enough and have demonstrated that they understand how to make good choices, they are allowed to cross the streets by themselves.

The same strategy can be used to help our young people gain the knowledge, skills, and motivation to use the Internet in a safe and responsible manner. We need to keep children in safe places on the Internet when they are very young. The use of filtering tools or the establishment of "safe places" can be helpful strategies at this stage. But we also must impart the values and skills that are the basis for the safe and responsible use of the Internet. As young people gain independence in their use of the Internet, we must teach them to how recognize potential unsafe situations and places and we must help them gain practical skills to handle the dangerous or tempting situations that may emerge when they use the Internet. Education, supervision, monitoring, and appropriate discipline are critically important during this stage.

Eventually, inevitably, young people will have unsupervised access to the Internet. We cannot prepare them for this eventuality by trying to keep them in a "safe place" using technology tools until they are 18 anymore than we could hope to protect a child from traffic by always holding onto his or her hand. We must focus our efforts on strategies that will empower young people with the values, knowledge, skills, and motivation to make the right choices in their behavior.

³ Oldenburg, A., "TV, Films blamed for child violence" *USA Today* July 26, p. 9D.

The focus of my work at the Center for Advanced Technology in Education, at the University of Oregon College of Education is to:

- Gain research insight about the behavior of young people when they are using the Internet.
- Develop and disseminate recommended policies, practices, and educational strategies to assist schools in helping young people engage in the safe and responsible use of the Internet.

What is the appropriate role of schools in teaching young people to make safe and responsible choices in the use of the Internet?

Schools must play a leading role in the effort to ensure that our young people learn to use the Internet in a safe and responsible manner. Schools are the most universal location where students in the U.S. are learning how to use the Internet. Not all parents know how to guide their children's use of the Internet, not all young people use the public library, not all young people have access through community technology centers. But schools have the ability to partner with parents, libraries, community technology centers, and other organizations within a community to create a community-wide effort to promote safe and responsible use of the Internet. Schools are a well-placed, efficient vehicle to provide education to parents on these issues.

Schools must establish guidelines for student use of the Internet that are in accord with educational standards. Schools cannot enforce a wide range of different family values. However, schools can and should encourage parents to engage in dialogue with their children about their personal and family values as they relate to their children's use of the Internet at school.

Is the use of filtering technology in schools the best way to address the safety and responsible use concerns?

The biggest problem with the use of filtering technology in schools is the false security and complacency that most often results from a decision to install filtering. When schools install filtering they often believe that they have adequately addressed safety and responsible use concerns related to the Internet. Schools that rely on filtering generally do not adequately address the search skills that young people can use to avoid inadvertently accessing this kind of material, nor do they discuss issues around the "darkside" of the Internet and the need to make responsible choices to avoid such material. Schools that rely on filtering often become complacent about supervision and monitoring, thus leading to other problems related to the use of the Internet. Often the choice to install filtering reflects inadequate dedication to professional development and Internet curriculum development⁴.

Most significantly, the concerns about safety and responsible use are more than simply concerns about the inadvertent or intentional access of potentially harmful material. Schools that rely on filtering generally are not addressing how their students will make safe and responsible choices in their behavior at those inevitable times when they will have unsupervised access through an unmonitored and unfiltered system.

The use of filtering in schools also raises first amendment concerns. These concerns are addressed in-depth in an accompanying document that outlines legal issues related to filtering in schools. In brief, school officials have the right and responsibility to determine the appropriateness of materials for their students, but may not restrict students' access to material based on a desire to suppress unpopular ideas. When school officials install filtering, they are delegating the responsibility for the determination of the appropriateness of materials to private companies that make blocking decisions based on vague criteria and

⁴ One administrator said to me, "We installed filtering because our teachers are not prepared to handle students' use of the Internet."

do not disclose their list of blocked sites to the schools. These companies are often found to have blocked sites presenting unpopular ideas in the same category as sites clearly are inappropriate for children, such as blocking access to information on safe sex or for gay and lesbian teens in the same category as pornography. Some companies have undisclosed agendas to use their filtering software to engage in viewpoint discrimination and suppress access to unpopular ideas.

Legislation currently pending in Congress that would require all schools receiving E-rate funds to install filtering will be held unconstitutional. Congress may not require that school officials entrust their important decision-making responsibility for the selection of school materials to private companies, especially given the significant deficiencies of today's filtering technologies.

Why would a school choose not to use filtering technology?

Schools that:

- **Have good policies and planning,**
- **Educate students about the importance of engaging in safe and responsible behavior,**
- **Engage students in high-quality educational uses of the Internet,**
- **Place the computers in locations where the monitors are easily visible, and**
- **Use effective supervision, monitoring and discipline strategies,**

do NOT have problems with students accessing inappropriate material.

The choice not to install filtering software in schools reflects the recognition of the important responsibility placed on schools to prepare young people to make the right choices and a determination that the use of filtering does not assist in achieving that objective. From a developmental perspective, technical monitoring systems are a far more powerful tool than are filtering systems. Monitoring systems place the responsibility on the young person for making the right choice and can detect when a wrong choice has been made. The detection can lead to a "teachable moment." This approach can be very helpful in helping young people learn to make decisions based on internalized control.

Here is how the Tom Ward, Principal of St. Michael School, Olympia, WA, described the rationale for his school's decision not to use filtering⁵:

"I feel that an assertive approach, works very well in every aspect of life, not just with a single medium. Therefore, an "Acceptable Use Agreement" for students, and staff, with clear, concise expectations outlined, will place the responsibility of each person's actions squarely on that person for his/her use the internet. Does that mean all have free reign? Absolutely not. The younger the child the more supervision and guidance is necessary.

The point is to not offer the easy way out by providing the excuse of "It's THEIR responsibility for what I do" but to instill the understanding that "I am responsible for the choices I make and I am accountable for what I choose to do". This is not only emphasized for a child's use of the net, but all forms of media during and outside of school.

⁵ Permission to reproduce and distribute this message was granted by the writer.

Education and community interaction not only occurs in school. It is important for youngsters to develop the need to make the right choices when they are NOT being "watched". Education is a life long process and our kids need to be able to function properly after 3:00 PM and after graduation. A youngster encouraged to develop a strong, value based character who can function independently and properly now will have the greater, more positive affect of influencing peers and raising the next generation than any outside control. ...

Educating our children is the best method of protecting them."

Here is a statement discussing an effective non-filtering-based strategy to address access to inappropriate sites by Rick Spitzer⁶, Director of Technology and Information Services, Widefield School District #3, Colorado Springs, CO.

"Our district does not filter. I randomly check a program that captures every URL requested in the district. In a day we may have 3000 to 5000 URLs requested. There are usually two to three inappropriate sites, and many of them are probably accidental. When we have observed problems they usually turn out to be adults. Sweepers, part time custodial help and so on are most likely because of times and locations. We deal with individuals and the students and staff know it.

All of our computers are in open areas and easily visible. The staff has been told to watch student activity and assign specific tasks.

Students and staff have been told that "You understand that the software you use tracks all "surfing" done on these computers. You also understand that your access privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken if you do not use the Internet in a responsible manner." In fact this is part of the browser startup screen on many district computers students use.

This does not guarantee that we do not have some problems or that we will not have problems in the future. Just as I cannot guarantee that there is not an adult magazine in our schools I cannot guarantee that a student has not see pornography on our computers. My observation at this point is that it is not worth the cost of the filtering software and the manpower required to do filtering. Students should be taught that this stuff is out there and if they run into it hit the Back button and move on. As long as that holds I will spend our technology funds on other more pressing issues."

Unfortunately, in the rush to find the simple solution -- a "technology tool" -- many schools have forgotten that education, supervision, and appropriate discipline are far more effective approaches to help young people learn how to behave in safe and responsible ways.

How should schools address concerns about the safe and responsible use of the Internet by young people?

Schools must address all issues related to the safe and responsible use of the Internet by young people. This includes all of the safety and wellbeing issues, as well as the responsible use issues outlined above.

The important foundation for the safe and responsible use of the Internet is:

- Teachers who are prepared to lead students in exciting, challenging, high-quality learning activities using the Internet.

⁶ Permission to reproduce and distribute this message was granted by the writer.

- A school environment that fosters responsible behavior and personal integrity throughout all aspects of school life.

The vast majority of school districts have adopted Internet Use Policies, also called Acceptable Use Policies, to guide student and staff use of the Internet⁷. The Internet use policy essentially establishes the "rules" for use of the Internet. Internet Use Policies address a wide range of safety and responsibility issues, including personal safety, illegal activities, system security, inappropriate language, privacy, resource limits, plagiarism, copyright infringement, as well as access to inappropriate material. If a student violates the provisions of an Internet use policy, he or she can be subjected to a range of disciplinary actions in accord with the district's disciplinary guidelines. A frequently used disciplinary action is denial of access to the Internet for a period of time. Internet Use Policies also address issues of students' rights in the context of their use of the Internet at school. These rights include the right of free speech, access to information, and due process. It is also important to establish the clear understanding that the use of the Internet in school is limited to educational purposes -- class assignments, career development, and high quality personal research, and not entertainment or shopping

A representative sample of a district Internet Use Policy as well as a detailed legal analysis of Internet use policy issues that was recently published in the Brigham Young University Journal of Law and Education have been attached.

The Internet Use Policy should only be considered the first component of a comprehensive strategy to assist young people in gaining the knowledge, skills, and motivation to use the Internet in a safe and responsible manner. A comprehensive strategy will address environmental and technical factors, instructional objectives and strategies, and intervention strategies.

It is my recommendation to educators that they develop a plan of action to address the safe and responsible use of the Internet. The overall plan initially should be developed at the district level in partnership with the representatives from the local public library, local community technology centers, and parent leaders. This overall plan must be refined at each school level to reflect the different facilities and needs of students at those schools.

To develop such a plan of action will require that educators have a greater understanding of the issues and concerns involved in addressing the safe and responsible use of the Internet by young people. Educators also must have an understanding of how the use of information technologies can affect how young people make decisions about their behavior. Educators need access to information about strategies that other schools are using to effectively address issues of concern. Currently, information and resources are not readily available to educators.

What are the best strategies for schools to address concerns of students accessing the "darkside" of the Internet?

Schools must do more than simply control student's use of the Internet during school hours. Schools must help students learn to make good choices in their use of the Internet at all times -- in school or not, supervised or not, filtered or not. To successfully address concerns about access to and engagement in the "darkside" of the Internet, it is necessary to distinguish between inadvertent access and intentional access. The former is a safety issue; the latter is a responsibility issue.

Inadvertent access of "darkside" sites can occur in several ways: a) conducting a search on an innocuous term that results in the presentation of a site with inappropriate material and accessing that site without a

⁷ A recent survey conducted by Quality Education Data revealed that in 1999 over 90% of school districts had adopted Acceptable Use Policies.

careful consideration of the description provided by the search engine; b) mistyping a URL; and c) selecting a link on a page when there is no description for the link or without reading the description. A school-based strategy to prevent the inadvertent access must begin when children begin to use the Internet. The foundation of an approach to avoid inadvertent access is to encourage students to "Read, Think, then Click." Unfortunately, many edutainment software programs for young children reinforce "mindless clicking," a bad habit that must be undone. Children must be warned of the presence of material on the Internet that is unacceptable for them to access. They must be provided with instruction in effective search strategies and learn how to quickly exit inappropriate sites, especially sites that have set "traps."

Children must be kept in child-safe places until they have successfully demonstrated that they understand how to avoid the inadvertent access of inappropriate material and how to quickly exit an inappropriate site. Child-safe spaces can be established through the use of portals or school web sites that are child-friendly, non-commercial, and educationally oriented.

Addressing the concern of intentional access to "darkside" sites and engagement in "darkside" activities is more complicated. To address issues of intentional access it is important to understand the range of motivations that may underlie intentional access. Many young people will access the "darkside" of the Internet because of curiosity. No creature is more curious than a teenager -- especially if adults are making a fuss about something. Most young people will explore the "darkside" of the Internet just to see for themselves what is there. Young people who find that the material is not consistent with their values will self-censor. Some of this exploration is simply a natural component of a young person's emerging sexuality. This kind of exploration has been present long before the Internet and cannot be expected to diminish when such materials are more readily available. The most important strategy to address concerns about curious teens is a focus on personal values, including healthy sexual values.

Some teens are part of peer group -- a "tribe" -- that reinforces ongoing involvement with "darkside" sites and activities during the period of teen age and young adult years. Given the strength of peer influences in the life of teens, early intervention in fostering positive teen tribes and assisting young people in resisting peer pressure to engage in activities that are contrary to their values are important prevention strategies.

The teens that present the greatest concern are those who engage in continued, excessive participation in "darkside" sites and activities and those who become victims of sexual predators or hate group recruiters. The teens who are likely to be most at-risk are those who perceive themselves to be outcasts in the school environment and those who have come from dysfunctional families where they have been the victims of emotional, sexual and/or physical abuse. Some at-risk teens may become involved in the establishment of "darkside" sites and may engage in online predation, harassment, and stalking. Their online involvement may also translate into "real world" activities of rape, sexual predation, stalking, domestic violence, and other illegal activities. Other at-risk teens may become the victims of online predators or recruiters. Teens who do not have "real world" connections with loving and caring adults and healthy peer relationships are the most receptive to the online grooming behavior of predators and recruiters. Clearly, there is a need for greater research insight to address the concerns presented by these at-risk young people.

"You are not old enough to look at this material," is an extremely weak argument against the "darkside". Such an argument will likely be dismissed by most teens, who consider themselves to be every bit as competent and capable as adults. The argument that they are not old enough flies in the face of the messages they have been receiving from the marketing moguls of the vast entertainment industry. It is probable that we will have much greater success in reaching young people if we focus the greatest amount of attention on the sites that contain violence and abuse and label these sites as such. The argument that "these sites foster violence and abuse" will likely be much more powerful than "you are not old enough." We also need to impart to young people an understanding of how viewing of and participation in violence and abuse activities can affect their perceptions, values, and behavior.

To lay the groundwork for success in fostering the safe and responsible use of the Internet, it is necessary that schools have well-developed programs addressing media literacy, character education, at-risk students,

racial discrimination, and sexual harassment. These programs can provide an essential foundation for imparting the values that are necessary to support safe and responsible behavior online.

Media literacy program will help young people develop skills in discerning when others are trying to manipulate their attitudes and exploit them. Unfortunately, the marketing techniques used by many of the dot.com sites aimed at children have the potential to undermine efforts to empower children to avoid unsafe activities and situations on the Internet. The marketing techniques used by legitimate dot.com companies are the same as those used by those who would recruit our young people to "darkside" sites and abusive activities. Here is an example: X is using the Internet to solicit personal information from a young person. X will use this information to develop a one-to-one relationship with the young person for the purpose of influencing the young person's attitudes and behavior. Did this describe a sexual predator, a hate group recruiter, a scam artist, or a dot.com children's site? The techniques described are used by "all of the above." We must assist young people in understanding when such techniques are being used to manipulate and exploit them. Media literacy programs can address these issues.

Character education programs seek to impart good values to young people. One potential problem with many character education programs is that they are frequently rule and punishment based. On the Internet, inappropriate behavior frequently goes undetected and, thus, unpunished. When working with young people using the Internet it is important to keep in mind how features of the technology can impact ethical decision-making. As young people grow, their ethical decision-making is largely influenced by external factors. The two most significant external forces are perception of the harm they have caused by their actions, which leads to feelings of guilt and remorse, and fear of detection, which could lead to punishment or loss of reputation. Technology interferes with both of these external forces. When we use technology, we are distanced from recognizing any harm that we may cause. We also feel invisible. As young people are growing up using the Internet, we must enhance their recognition of potential harm caused by their actions and diminish their perceptions that they are invisible. Our character education programs must focus their attention on enhancing internalized control through an understanding of how our actions can cause harm to unseen others.

Students who are determined to be at-risk for other behavioral problems, especially the school "outcasts," are also the ones who are most at-risk of becoming involved in "darkside" activities on the Internet. Educators must recognize that any student who does not feel a part of the school community is likely to be finding an online community or an individual predator ready and willing to exploit his or her loneliness. Helping students feel connected and cared for in their home, school, and community takes on even greater importance in recognition of the potential that young people who do not feel connected and cared for are extremely vulnerable on the Internet.

With the growth of hate sites on the Internet, it is evident that schools need to address issues related to hate materials and hate group recruitment in school-based programs that address racial discrimination. Many hate sites are using sophisticated communication techniques and creating well-designed web sites that provide a façade of legitimacy. Young people need the knowledge and skills to recognize hatred and disrespect regardless of the form in which it is presented online.

In 1993, the American Association of University Women published a peer sexual harassment study. The study showed that 81% of students had experienced some form of sexual harassment. Eighty-five percent of girls and 76 percent of boys reported experiencing 'unwanted and unwelcome sexual behavior that interferes with their lives.'⁸ The values and attitudes of students that underlie involvement in peer sexual harassment are likely to be the same values and attitudes that support intentional involvement with the sexual "darkside" of the Internet. Aggressive school-based programs to address sexual harassment are likely to provide an effective foundation for addressing involvement with sexual "darkside" materials on the Internet.

⁸ American Association of University Women Educational Foundation, *"Hostile Hallways: The AAUW Survey on Sexual Harassment in American Schools"* June 1993.

What should be done?

The following are some practical, proactive recommendations:

- Encourage school districts and schools to develop a plan of action to address how they will assist students to engage in the safe and responsible use of the Internet. Schools should work with parents, public libraries, and community technology centers to develop a comprehensive, community-wide approach. This approach will move schools beyond the simple adoption of an Internet Use Policy. School districts and schools will need support for this planning through the provision of information about the issues of concern and access to recommendations for effective strategies. (If Congress is intent on enacting legislation to address these concerns, a requirement for such a plan could be added to the requirements necessary for funding through the E-rate program.)
- Develop a comprehensive taxonomy of educational objectives related to the safe and responsible use of the Internet. Providing guidelines for learning objectives that are appropriate for different grade levels. This taxonomy should provide the basis for the development of curriculum materials and approaches.
- Provide professional development for teachers and administrators regarding safety and responsible use issues.
- Support research to gain a better understanding of how use of the Internet is affecting the social and moral development of young people and to understand how to assist young people in engaging in the safe and responsible use of the technology.
- Revise media literacy, character education, at-risk, racial discrimination, and sexual harassment curriculum programs to incorporate concepts necessary to support making safe and responsible choices using the Internet.

Conclusion

Dr. Suess provided excellent guidance on this issue. In his book *Oh the Places You'll Go!* he wrote:

"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."⁹

The answer to our concerns about the "darkside" of the Internet is to focus on strategies that can help our young people gain those "heads full of brains and shoes full of feet" so that they **choose** not to go down those not-so-good cyberstreets.

⁹ Suess, Dr. *Oh, the places you'll go!* New York: Random House. 1990.