

Cyberbullying, Cyberthreats, and Dangerous Online Communities

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Use of the Internet
Web sites: <http://csriu.org> and <http://cyberbully.org>
E-mail: nwillard@csriu.org
© 2005, 06 Nancy Willard
Permission to reproduce and distribute
for non-profit, educational purposes is granted.

Cyberbullying

- Cyberbullying is being cruel to others by sending or posting harmful material or engaging in other forms of social cruelty using the Internet or other digital technologies.
- Cyberbullying can take different forms, including:
 - Flaming. Online “fights” using electronic messages with angry and vulgar language.

Joe and Alec’s online fight got angrier and angrier. Insults were flying. Joe warns Alec to watch his back in school the next day.
 - Harassment. Repeatedly sending offensive, rude, and insulting messages.

Matt reported to the principal that students were bullying another student. When Matt got home, he had 35 angry messages in her email box. The anonymous cruel messages kept coming—some from total strangers.
 - Denigration. “Dissing” someone online. Sending or posting cruel gossip or rumors about a person to damage his or her reputation or friendships.

Brad’s blog is filled with racist profanity. Frequently, he targets black and Latino student leaders, as well as minority teachers, in his angry verbal assaults.

Middle school students created a web site denigrating Raymond. They posted stories, jokes, and cartoons ridiculing his size and questioning his sexual orientation.
 - Impersonation. Breaking into someone’s account, posing as that person and sending messages to make the person look bad, get that person in trouble or danger, or damage that person’s reputation or friendships.

Laura watched closely as Emma logged on to her account and discovered her password. Later, Laura logged on to Emma’s account and sent a scathing message to Emma’s boyfriend, Adam.
 - Outing and Trickery. Sharing someone’s secrets or embarrassing information or images online. Tricking someone into revealing secrets or embarrassing information, which is then shared online.

Sitting around the computer with her friends, Judy asked, “Who can we mess with?” Judy started IM-ing with Sara, asking her many personal questions. The next day, the girls were passing around Sara’s IM at school.

Greg, an obese high school student, was changing in the locker room after gym class. Matt took a covert picture of him with his cell phone camera.

Within seconds, the picture was flying around the cell phones at school.

- Exclusion. Intentionally excluding someone from an online group, like a “buddy list.”

Millie tries hard to fit in with group of girls at school. She recently got on the “outs” with a leader in this group. Now Millie has been excluded from the IM “buddy” lists and friendship links of all of the girls.

- Cyberstalking. Repeatedly sending messages that include threats of harm or are highly intimidating. Engaging in other online activities that make a person afraid for her or her safety.

When Annie broke up with Sam, he sent her many angry, threatening, pleading messages. He spread nasty rumors about her to her friends and posted a sexually suggestive picture she had given him in a sex-oriented discussion group, along with her email address and cell phone number.

Cyberthreats

- Cyberthreats are either direct threats or distressing material that raises concerns or provides clues that the person is emotionally upset and may be considering harming someone, harming him or herself, or committing suicide.

Jeff comments in his blog: “I’m a retarded [expletive] for ever believing that things would change. I’m starting to regret sticking around. It takes courage to turn the gun on your self, takes courage to face death.” Later he wrote: “Things are kind of rocky right now so I might disappear unexpectedly.

Celia met Andrew in a chat room. Andrew wrote: “bring a gun to school, ur on the front of every ... i cant imagine going through life without killing a few people ... people can be kissing my shotgun straight out of doom ... if i dont like the way u look at me, u die ... i choose who lives and who dies”

- Relationship to cyberbullying.
 - Sometimes cyberbullying will reach the level of a direct threat.
 - Sometimes cyberbullying will lead the target to make distressing comments.

A group of girls at his school had been taunting Alan through instant messaging, teasing him about his small size, daring him to do things he couldn’t do, suggesting the world would be a better place if he committed suicide. One day, he shot himself. His last online message was, “Sometimes the only way to get the respect you deserve is to die.”

Dangerous Online Communities

- “At risk” youth are attracted to dangerous online communities.
 - Depressed or angry teens who have personal difficulties and/or problems in relationships with family, school, and/or peers are extremely vulnerable online because they are “searching for love in all the wrong places.”
- There appear to be two forms of dangerous online communities.
 - Self-formed communities—youth who share feelings of disassociation who find and establish informal groups that engage in discussions. May include communities in social networking sites or independent web sites. Types of communities include:
 - Suicide communities.

Jason was depressed and suicidal. He made plans for his suicide in

conjunction with an online group of other depressed individuals he considered his friends. One evening, with his web cam running, he took an overdose. His online group communicated with him until he was no longer able to communicate—and then just watched him die.

- Self-harm communities, including cutting, anorexia, and passing out.
- Troublesome youth groups—school or community-based informal “gangs” of outcasts.

Five students from a high school were using a social networking site to discuss plans to conduct an armed attack on their school to commemorate the anniversary of Columbine.

- More formal dangerous organizations
 - Distinguished from informal communities because they have adult members and engage in specific recruitment.
 - Hate groups and gangs.
- Involvement in dangerous online communities can lead to contagion— adoption of unsafe, dangerous attitudes and inclinations to engage in unsafe, dangerous activities.

You Can't See Me. I Can't See You

- Why is it that when people use the Internet or other technologies, they sometimes do things that they would never do in the “real world?”
 - You Can't See Me. When people use the Internet, they perceive they are invisible. The perception can be enhanced because they create anonymous accounts. People are not really invisible, because online activities can be traced. But if you think you are invisible, this removes concerns of detection, disapproval, or punishment.
 - I Can't See You. When people use the Internet they do not receive tangible feedback about the consequences of their actions, including actions that have hurt someone. Lack of feedback interferes with empathy and leads to the misperception that no harm has resulted.
 - Everybody Does It. The perception of invisibility and lack of tangible feedback support risky or irresponsible online social norms, including:
 - “Life online is just a game.” Allows teens to ignore the harmful “real world” consequences of online actions and creates the expectation that others will simply blow off any online harm.
 - “Look at me—I'm a star.” Supports excessive disclosure of intimate information and personal attacks on others, which may be done for the purpose of attracting attention.
 - “It's not me. It's my online persona.” The ability and inclination of teens to assume online personas or other identities allows teens to deny responsibility for actions taken by one of these personas or identities.
 - “What happens online, stays online.” Supports the idea that teens should not bring issues related to what has happened online into the “real world” and should not disclose online activity to adults.
 - “On the Internet, I have the free speech right to write or post anything I want regardless of the harm it might cause to another.” Supports harmful speech and cruel behavior as a free speech right.
- We need to educate students about the limits on “free speech.”
 - Sources of those limits include:

- Family and spiritual values.
 - School rules.
 - Terms of use agreements of Internet service providers, web sites, and cell phone companies.
 - Civil law standards. Cyberbullying could meet standards for defamation, invasion of privacy by disclosure of private fact, false light, or intentional infliction of emotional distress.
 - Criminal law. Cyberbullying could be in violation of criminal law including, threats of violence, harassment or stalking, hate or bias crimes, material harmful to minors, child pornography, or sexual exploitation, or taking photo in private place.
 - Personal values. Most important limit. Teens are in the process of solidifying their personal values.
- We also need to help students learn how to make more ethical choices online.
 - Questions that encourage a focus on ethical standards include:
 - “Is this kind and respectful to others?”
 - “How would I feel if someone did the same thing to me, or to my best friend?”
 - “What would my mom, dad, or other trusted adult think or do?”
 - “Would I violate any agreements, rules, or laws?”
 - “How would I feel if my actions were reported on the front page of a newspaper?”
 - “What would happen if everybody did this?”
 - “Would it be OK if I did this in person, or in the “real world?”
 - “How would this reflect on me?”

How and Who

- There is insufficient high quality academic research of these concerns to draw any strong conclusions about these concerns. All of the following insights are based on observation and anecdotal reports.
- Cyberbullying or cyberthreat material—text or images—may be posted on personal web sites or blogs or transmitted via email, discussion groups, message boards, chat, IM, or cell phones.
 - Frequently, such material is being posted on or sent through social networking sites. Social networking sites, like MySpace and Xanga, are highly popular with middle and high school students. The sites allow students to establish a profile and web page, link to friends, communicate with friends through comments posted on the sites, in blogs, through private messages or instant messaging, and in discussion groups.
 - Most of these sites and services have terms of use that prohibit posting harmful material and will respond by removing such harmful content and terminating the membership of the offending poster. Safe school personnel, parents, and bully targets should know that they can file a complaint to have the material removed.
- A significant amount of the cyberbullying activity is occurring off-campus, but is impacting student relationships on-campus. But it is also highly likely that in many schools, students are using the district Internet system or personal cell phones to engage in cyberbullying.
 - Internet filtering systems are totally ineffective in preventing student misuse of the Internet to engage in cyberbullying. Students can easily bypass any Internet filter.

- A cyberbully or person posting a direct cyberthreat is generally a person whom the target knows.
 - But a student who wants to target another student may also solicit involvement of other people who do not know the target—cyberbullying-by-proxy.
 - Or the cyberbully or person posting a cyberthreat may be anonymous or could impersonate someone else.
 - Generally, teens are not very good at hiding their identity. Investigations of other material posted, friendship links, and interviews with less-involved students will generally allow identification. Law enforcement officials have greater ability to obtain identity information.
- Cyberbullying incidents and cyberthreats are frequently related to in-school bullying.
 - Sometimes, the student who is victimized at school is also being bullied online.
 - But other times, the person who is victimized at school retaliates online.
 - Other times, the student who is victimized at school will share his or her anger or depression online as distressing material or a direct threat.
 - It is imperative that school officials understand these dynamics and not immediately assume that the student posting the harmful online material is the originator of the problem. The best way to figure this out is to look at the “social status” level of all of the participants. If a student who has posted harmful online material is considered to be a “loser” or is an “outcast” at school or is at the social status level lower than the individual targeted it is highly probable that this material is posted in retaliation for bullying or other harm inflicted at school.
 - It appears that the students most often involved in cyberbullying are the “in-crowd” students, with the “wannabes” the most frequent targets. These are the students who are participating with each other in online groups.
 - Students who are less inclined to participate actively in the social dynamics of school tend to form their own online groups, which could simply be independent groups or dangerous groups. This spring, there appears to have been a significant increase in reports of groups of 5 or 6 male students, who appear to be “outcasts,” who have been found to be using the Internet to plan school violence.
- Cyberbullying may involve personal relationships.
 - If a relationship breaks up, one person may start to cyberbully the other person.
 - Other times, teens may get into online fights about relationships.
 - Sometimes, teens provide intimate images to others in the context of relationships—and upon a break-up, this material could be disseminated.
- Cyberbullying may be based on hate or bias—bullying others because of race, religion, obesity, or sexual orientation. Cyberbullying based on sexual orientation appears to be quite frequent and has been implicated/suggested in most of the cases that have resulted in suicide.
- Teens may think that cyberbullying entertaining—a game to hurt other people. This may be related to online role-playing gaming involvement.
- If students have been actively socializing online, it is probable that they have been involved in cyberbullying in one or more of the following roles:
 - Bullies.

- “Put-downers” who harass and demean others, especially those they think are different or inferior.
 - “Get-backers” who have been bullied by others and are using the Internet to retaliate or vent their anger.
- Targets. The targets of the cyberbully.
- Harmful Bystanders. Those who encourage and support the bully or watch the bullying from the sidelines, but do nothing to intervene or help the target.
- Helpful Bystanders. Those who seek to stop the bullying, protest it, provide support to the target, or tell an adult. We need more of these kinds of bystanders!
- Students are also posting harmful material targeting teachers or other staff.
 - Sometimes this appears to be “youthful exuberance,” a convenient target, and a lack of sensitivity to the harm caused.
 - Other times, the staff person is targeted because of some perceived status issue, such as sexual orientation or obesity.
 - Some cases may involve situations where the student legitimately feels that he or she has been bullied or mistreated by the teacher.
 - Sometimes, student post totally legitimate objections to the actions or policies of the school or school staff.

The Impact of Cyberbullying

- It is widely known that face-to-face bullying can result in long-term psychological harm to targets. This harm includes low self-esteem, depression, anger, school failure, school avoidance, and, in some cases, school violence or suicide. It is possible that the harm caused by cyberbullying may be even greater than harm caused by traditional bullying because:
 - Online communications can be extremely vicious.
 - There is no escape for those who are being cyberbullied—victimization is ongoing, 24/7.
 - Cyberbullying material can be distributed worldwide and is often irretrievable.
 - Cyberbullies can be anonymous and can solicit the involvement of unknown “friends.” The target may not know who he or she can trust.
 - Teens may be reluctant to tell adults what is happening online or through their cell phone because they are emotionally traumatized, think it is their fault, fear greater retribution, or fear online activities or cell phone use will be restricted.
- There are reports of cyberbullying leading to suicide, school violence including one school murder, and many reports of cyberbullying leading to school failure and avoidance.

Cyberthreat Issues

- Youth make threats. Their tone of voice, posture, overall interaction allow others to determine whether or not their expression is a “real threat.”
 - Online material that looks threatening could be:
 - A joke, parody, or game.
 - A rumor that got started and has grown and spread.
 - Material posted by a young person who is trying out a fictitious threatening online character.
 - The final salvos of a “flame war” that has gotten out of hand, but will unlikely

- result in any real violence.
 - Material posted by someone impersonating another someone else for the purpose of getting that person into trouble.
 - Distressing material posted by a depressed or angry young person that could foretell a violent or suicidal intention, but does not represent an imminent threat.
 - A legitimate imminent threat.
 - Obviously, school officials must respond to a possible threat in the most appropriate manner, based on the available information. But a rapid investigation and continuous reassessment of the situation is necessary.
 - It is really important to communicate two messages to youth about cyberthreats.
 - Don't post material that an adult might perceive to be a threat.
 - Report any material that appears to be a threat, because it is better to risk a report that turns out to be false than real harm.
- "Leakage" occurs when a student intentionally or unintentionally reveals clues to feelings, thoughts, fantasies, attitudes, or intentions that may signal an impending violent act against self or others.
 - Schools should assume that emotional distraught youth with Internet access will be posting material that provides significant insight into their mental state.
 - Frequently, these comments will be posted on a student's profile or web site on an online social networking site.
- The fact that cyberbullying or cyberthreat material is or can be preserved in electronic format, and the true author can generally be identified, provides some significant advantages for savvy safe school personnel to more effectively discover and intervene in these incidents.

Celia, the student described in a cyberthreats story, saved the chat with Andrew, gave it to her father, who contacted the police, who conducted a search and found that Andrew was a member of a hate group and had many weapons, including an AK-47. The threat was found to be legitimate and Andrew is now in prison.

Legal Issues

- Search and seizure—When can a school monitor and search student Internet use records and files?
 - Apply the “locker search standard” to Internet use.
 - Users have a limited expectation of privacy on the district's Internet system.
 - Routine maintenance and monitoring, (technical and by staff) may lead to discovery that a user has violated district policy or law.
 - An individual search will be conducted if there is reasonable suspicion that a user has violated district policy or the law.
 - Schools should determine who has authority to authorize individual search and record-keeping.
 - Clear notice can enhance deterrence.
- Free speech issues—When can a school respond to cyberbullying?
 - The First Amendment places restrictions on public officials when intervening in situations involving expression of speech by students, especially off-campus.
 - *Tinker* standard. School officials may intervene only when there is a substantial and material threat of disruption or interference at school or with the rights of

- other students to be secure.
- Has recently been applied to off-campus online speech by students that relates to the school.
 - But some legal commentators disagree with the application of *Tinker* to any off-campus speech by students.
- *Hazelwood* standard. School officials may impose educationally-based restrictions. Applies to on-campus speech that occurs through a school-authorized forum, such as school newspaper.
 - Should apply to speech disseminated through district Internet system and campus use of cell phones.
 - Off-campus online harmful speech cases.
 - Almost all cases involved speech directed at school staff.
 - In almost all cases, the districts have lost or settled, despite really awful online material.
 - In one case, the district won because the student had accessed the site from school and the teacher was very emotionally upset.
 - There are no cases addressing school discipline for really serious harmful online speech directed at a student. Unfortunately, schools appear more inclined to punish students for material that targets staff.
 - If off-campus online speech of a student has caused a material and substantial disruption in the life of another student and the ability of that student to fully participate in school, can the school respond? Probably—but the legal standards are unclear.
 - To address situations, search diligently for an actual school “nexus” to bring case under *Hazelwood* standard or evidence to establish that there is a substantial disruption (or threat) to strengthen the justification for a school response under the *Tinker* standard. Look for the following:
 - Material posted or sent through district Internet system—review use records.
 - Material displayed to other students through district Internet system.
 - Material originated on-campus, like a photo taken with a cell phone.
 - Relationship of material posted online to on-campus bullying.
 - Emotional harm suffered by student and interference with this student’s right to feel secure and be successful at school.
 - Other school disruptions or possible school disruptions.

Several high school students, one of whom was African-American, were engaged in a school altercation, which the principal thought he had resolved. Soon thereafter, the two Caucasian students created a page on a social networking site where they posted pictures and cartoons depicting lynching and dragging African American individuals behind cars. Other students from the school had found out about the site and had established links to it. The African-American student found out and told the African-American student organization. He also reported the site to the principal. The principal took the time to investigate by viewing and saving the materials and interviewing students who had linked to the site to ensure he had absolute knowledge of who the creators were. He suspended the students. (Within a day and without any staff leadership, other students in the school had hung posters declaring that racism was not accepted.) Was this Principal’s intervention and imposition of formal discipline legal justified? Clearly, yes.
 - If there are questions or concerns about the right to impose formal discipline, there are many steps an administrator can take to address the situation.

- Codes of conduct for extracurricular activities—Is it possible to expand the reach of *Tinker* by including prohibitions against harmful online speech in the codes of conduct for extracurricular activities?
 - Phrase this question another way: Can students be forced to give up their constitutional rights of free expression in order to participate in extracurricular activities? Probably not. It is likely the *Tinker* standard would still hold.
- District liability—When must a school respond to cyberbullying?
 - District liability concerns are raised when cyberbullying or cyberthreats are occurring through district Internet system or via cell phone on campus.
 - Negligence claim
 - Duty to protect. Duty to anticipate foreseeable dangers and take necessary precautions. Schools have a duty to exercise precautions against student cyberbullying through district Internet system and through use of cell phones on campus.
 - Failure to exercise a reasonable standard of care. How would a "reasonable" educator in a similar situation have acted? Has the district established a reasonable level of supervision/monitoring of student use of the Internet and provided a vehicle to report and respond to cyberbullying activity? Many districts have not established a reasonable level of monitoring and do not have effective reporting/response.
 - Proximate cause. Was the student's injury foreseeable? Was there as a connection between breach of duty and injury? Was it foreseeable that students could be using the district's Internet system to post to send harmful material to other students and did the lack of supervision/monitoring allow such an injury to occur? It is entirely foreseeable that students are using the district Internet system to cyberbully others, whether there is a connection will depend on facts
 - Actual injury. Was there a physical/emotional injury? Will depend on the facts.
 - Statutory liability.
 - Civil rights statutes.
 - Title IX of the Education Amendments of 1972.
 - Title VI of the Civil Rights Act of 1964.
 - State civil rights statutes.
 - A violation of Title IX and VI may be found if a school has effectively caused, encouraged, accepted, tolerated, or failed to correct a sexually or racially hostile environment of which it has actual or constructive notice.
 - A school is charged with constructive notice of a hostile environment if, upon reasonably diligent inquiry in the exercise of reasonable care, it should have known of the discrimination.
 - Is the district being reasonably diligent in ensuring that students are not using the district Internet system in a harmful manner?

Ebony, an African American sixth grade student, received an email while at school threatening that she would be harmed after her 8th period class and referencing the KKK. She showed this message to her teacher. Neither the teacher nor the school responded to the report of this email message. She was terrified and suffered significant emotional trauma.
 - My personal opinion is that the vast majority of schools are relying far too heavily on filtering software to seek to control Internet activities of students and that it is highly probable that students are using the district Internet system to cyberbully

others. Schools with 1:1 laptop programs are at highest risk. To avoid possible liability, in my opinion, schools must:

- Conduct a needs assessment to determine extent of problems related to misuse of the Internet and cell phones on campus.
- Revise policies and Internet use management practices.
- Implement more effective practices to monitor student Internet use.
- Educate students and teachers on the concerns of cyberbullying.
- Implement a cyberbullying report, review, and intervention process.

Comprehensive School and Community-based Approach to Address Cyberbullying and Cyberthreats

- The following is a “research-guided” approach.
 - Based on:
 - Best practices in bullying, violence, and suicide prevention programs.
 - Research insight into bullying.
 - Traditional threat assessment processes.
 - Combined with:
 - Insight into online behavior of youth.
 - Legal analysis.
 - Comprehensive approach to manage Internet use in school and home.
 - Not yet research-based. So it is essential to incorporate effective accountability practices. If using federal safe schools funds, must request waiver of Principles of Effectiveness
- Comprehensive planning through safe schools committee.
 - Members.
 - Administrator.
 - Counselor/psychologist.
 - Technology director.
 - Librarian.
 - Community members. School security officer, parents, law enforcement, mental health organizations
 - Students. Probably important, but potentially problematical because students could be viewed as traitors.
 - This approach will require a systemic change. Currently, technology services departments manage Internet use issues and safe schools committees address safe school issues. This separation cannot continue.
- Needs assessment—bringing “sunlight” to the problem.
 - Student survey to address:
 - On-campus or off-campus instances.
 - Relationship to on-campus actions.
 - Impacts.
 - Reporting concerns.
 - Attitudes, risk factors, and protective factors.
 - May need to be done first, to convince people that there is a real concern.
 - Conducting a regular survey can provide insight into the effectiveness of the program.
- Policy and practice review.
 - All safe school personnel must have the immediate ability to bypass the school's

- Internet filter to review material posted online on any site!
- Expand the bullying/threat report process to incorporate cyberbullying and cyberthreats.
 - Should be anonymous and/or confidential because concerns about online retaliation are very real.
 - Establish an online reporting form or email report.
 - Make sure students know to provide downloaded material and/or the URL where the harmful material has been found.
- Review cell phone/PDA policies and practices.
 - Misuse should lead to discipline for bullying and ban on device at school.
- Review Internet policies and practices.
 - See more below.
- Establish cyberbully or cyberthreat situation review and intervention plan.
 - See more below.
- The overall threat assessment process and suicide prevention planning processes should also address Internet communications
 - If any suggestion of threat is reported or a student appears to be distressed, it is advisable to search online for additional material and insight.
- Professional development.
 - “Triage” approach.
 - Key person in district/region/state needs high level of training.
 - Safe schools planning committee and all “first responders” need insight into problem and ways to detect, review, and intervene, with back-up from key person.
 - All other staff need general awareness.
 - All safe school personnel must know how to investigate online postings of students.
- Parent outreach.
 - Provide information on how to:
 - Prevent, detect and intervene if their child is victim.
 - Prevent their child from being cyberbully.
 - Possible consequences if child is a cyberbully.
 - Empower their child to be a responsible bystander.
 - Provide information to parents through:
 - General information through newsletters.
 - Parent workshops.
 - “Just-in-time” comprehensive resources in office and online because parents likely will not pay attention until they need the information.
- Community outreach.
 - Provide information and training to others:
 - Mental health professionals.
 - Faith-based organizations.
 - Youth organizations.
 - Public library and community technology centers.
 - Media.
- Student education.
 - Prerequisite to addressing cyberbullying is effective social skills education.

- Educational approach should foster internalized values and character and empowerment of victims and bystanders.
 - Enhance predictive empathy skills.
 - Teach ethical decision-making skills.
 - Teach conflict resolution and peer mediation.
- Enhance understanding of Internet safety and responsible use.
 - Cyberbullying prevention and responses.
 - Legal principles of online publishing.
 - Internet privacy and public disclosure concerns.
 - Reporting cyberthreats and not making cyberthreats.
- Evaluation and assessment.
 - Ongoing evaluation is critically important. Cyberbullying is an emerging concern in a new environment that is not fully understood.
 - Evaluation should inform implementation.
 - Performance measures approach.
 - Performance objectives – tie to needs assessment findings.
 - Inputs — resources allocated to the activities.
 - Activities — specific program activities or tasks.
 - Outputs — direct products of the program activities.
 - Outcomes — consequences of the program on the intended recipients.

Effective Internet Use Management

- The increased youth use of the Internet, especially social networking sites, is raising significant concerns about the effective management of Internet use in schools.
 - Continued reliance on filtering/blocking approaches is unwarranted.
 - Filters are not blocking access to all inappropriate material.
 - They can easily be bypassed by students. Google: “bypass, Internet, filter.”
 - They are blocking student access to constitutionally protected material.
 - A more effective approach is grounded in a strategy to:
 - Protect of elementary students by restricting Internet use to safe places and safe communications.
 - Empower middle and high school students to make safe and responsible choices through education and clear policies.
 - Limit the non-educational use of the Internet at school.
 - Implement effective supervision and monitoring practices, including technical monitoring.
- Planning and accountability.
 - Internet use management and safe schools planning must be integrated. This will require system change.
 - Regular assessment, including assessment of the educational use of the Internet and student (and staff) misuse, is essential.
- Education purpose.
 - Internet use in schools should be for educational purposes only. There is too much “Internet recess.”
 - Classwork and independent research on subjects similar to what studied in school or resources in library.
 - This is necessary preparation for workplace. Internet use on the job should also be for work-related purposes only.

- Increased professional and curriculum development in effective, high quality use of technology is essential to ensure focus on educational activities.
 - Restricting “Internet recess” will be difficult in some schools because this will require restricting freedoms that are now expected.
- Internet use policies and practices.
 - Policies.
 - Revisit policies to ensure they are up-to-date.
 - Policies must be clearly communicated to staff and students through signage in computer labs and during sign-on.
 - Establish “safe boundaries” for elementary students.
 - Previewed sites.
 - Controlled communications.
 - Establish guided resources for middle and high school students.
 - Allow explorations outside of guided boundaries for specific projects.
 - Controlled communications, including blogs and wikis.
 - Provide access to reviewed sites for sensitive health information that will not be blocked or monitored.
- Student, parent, staff education.
 - Student education .
 - Focus on knowledge, skills, and values.
 - Incorporated into health or technology classes in middle and high school.
 - Use “teachable moments,” such as related lessons or recent news stories.
 - Parent education.
 - Schools can be effective conduit to parents.
 - Major problem is that the parents who really need the information are the least likely to take advantage of opportunities to obtain information.
 - Seek to use a variety of approaches, including information in newsletters, workshops, and information available in school office, health room, counselor’s office and online.
 - Staff Education.
 - Staff who work with students who are using computers, including substitute teachers, must understand the risks and know effective management and monitoring practices.
- Effective Monitoring.
 - Must shift from “blocking” approach to effective “monitoring.”
 - Supervision of students by teachers is essential. Having students provide their printed history file is one strategy.
 - Technology-facilitated monitoring, including intelligent content analysis of Internet traffic, is strongly advised.
- Appropriate Discipline.

Cyberbully or Cyberthreat Situation Review and Intervention

- See attached.

Nancy E. Willard has degrees in special education and law. She taught “at risk” children, practiced computer law, and was an educational technology consultant before focusing her professional attention on issues of youth behavior when using information and communication technologies. Nancy frequently conducts workshops for educators. She is expanding her use of Internet technologies to deliver “virtual” presentations and classes. This material is adapted from her new book *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Cruelty, Threats, and Distress*.