Educator's Guide to Cyberbullying and Cyberthreats

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Use of the Internet

Author of *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress* (Research Press) and *Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn to Use the Internet Safely and Responsibly* (Jossey-Bass)

Web sites: http://csriu.org, http://cyberbully.org, and http://cyber-safe-kids.com
E-mail: nwillard@csriu.org

April 2007

Young people have fully embraced the Internet as both an environment and a tool for socializing. Via the Internet and other technologies, they send e-mail, create their own Web sites, post intimate personal news in blogs (online interactive journals), send text messages and images via cell phone, contact each other through IMs (instant messages), chat in chat rooms, post to discussion boards, and seek out new friends in teen sites.

Unfortunately, there are increasing reports of teenagers (and sometimes younger children) using these technologies to post damaging text or images to bully their peers or engage in other aggressive behavior. There are also increasing reports of teens posting material that raises concerns that they are considering an act of violence toward others or themselves.

This guide provides educators with insight into these concerns and guidelines to prevent and respond. This guide provides only a brief overview of these concerns. More information, as well as implementation documents, is available in *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress* (Research Press)

CYBERBULLYING

Cyberbullying is being cruel to others by sending or posting harmful material or engaging in other forms of social aggression using the Internet or other digital technologies. Cyberbullying can take different forms:

- **Flaming.** Online fights using electronic messages with angry and vulgar language.

  Joe and Alec's online exchange got angrier and angrier. Insults were flying. Joe warned Alec to watch his back in school the next day.

- **Harassment.** Repeatedly sending nasty, mean, and insulting messages.

  Sara reported to the principal that Kayla was bullying another student. When Sara got home, she had 35 angry messages in her e-mail box. The anonymous cruel messages kept coming—some from complete strangers.

- **Denigration.** "Dissing" someone online. Sending or posting gossip or rumors about a person to damage his or her reputation or friendships.

  Some boys created a "We Hate Joe" Web site where they posted jokes, cartoons, gossip, and rumors, all dissing Joe.

- **Impersonation.** Pretending to be someone else and sending or posting material to get that person in trouble or danger or to 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 hurtful message to Emma's boyfriend, Adam.

- **Outing.** Sharing someone's secrets or embarrassing information or images online.

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

- **Trickery.** Talking someone into revealing secrets or embarrassing information, then sharing it online.

  Katie sent a message to Jessica pretending to be her friend and asking lots of questions. Jessica responded, sharing really personal information. Katie forwarded the message to lots of other people with her own comment, "Jessica is a loser."

- **Exclusion.** Intentionally and cruelly excluding someone from an online group.

  Millie tries hard to fit in with a group of girls at school. She recently got on the "outs" with a leader in this group. Now Millie has been blocked from the friendship links of all of the girls.

- **Cyberstalking.** Repeated, intense harassment and denigration that includes threats or creates significant fear.

  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 e-mail address and cell phone number.

CYBERTHREATS

Cyberthreats are either direct threats or "distressing material"—general statements that make it sound like the writer is emotionally upset and may be considering harming someone else, harming himself or herself, or committing suicide.

Jeff wrote 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." Jeff was also sharing his plans for an attack with a friend via e-mail.

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 . . . if i dont like the way u look at me, u die . . . i choose who lives and who dies"

Greg set up an anonymous IM account and sent a threatening message to his older sister suggesting that she would be killed the next day at school.

Just in case you are wondering—these are all true stories. Jeff killed nine people and then killed himself. Celia reported her online conversation to her father, who contacted the police. The police found that Andrew had many weapons, including an AK-47. He is now in prison. Greg's sister told her parents, her parents told the school, and the school went into "lockdown." Greg was identified easily—and arrested for making a threat.

School officials must recognize that what initially appears to be an online threat can be any of the following:

- 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.

The problem is that when school officials or law enforcement are first appraised of an online threat, it may be difficult to tell which of the above possibilities might be involved. Obviously, the highest priority is doing what is necessary to protect against a possible legitimate threat. But processes also must be in place to rapidly determine the legitimacy of the threat. Sometimes when teens post what appears to be a threat, they are just joking. One important message to communicate to students is:

- **Don't make threats online.** If you post a threat online, adults may not be able to tell whether the threat is real. There are criminal laws against making threats. If you make a cyberthreat, even if you are just joking, you could be suspended, expelled, or even arrested.

The other problem is that adults are generally not present in online communities where such material is being posted. There are other very important message to students is:

- **Report threats or distressing material.** If you see a threat or distressing material posted online, it could be very real. It is extremely important to report this to an adult. If the threat is real, someone could be seriously injured.

HOW, WHO, AND WHY

Cyberbullying or cyberthreat material—text or images—may be posted on personal Web sites or blogs or transmitted via e-mail, discussion groups, message boards, chat, IM, or cell phones.

Students are engaging in this activity outside of school—but because the participants are also together in school, this off-campus activity may be impacting the school climate or interfering with the ability of students to be successful in school. Students are also engaging in this activity while using the district Internet system, while in school or when off-campus if access to the district Internet system is allowed, or when using personal digital devices, including cell phones, PDAs or personal laptops, while on campus.

A cyberbully may be a person whom the target knows or an online stranger. Or the cyberbully may be anonymous, so it is not possible to tell. A cyberbully may solicit involvement of other people who do not know the target—cyberbullying by proxy.

> *Sue convinced Marilyn to post anonymous comments on a discussion board slamming Kelsey, a student she had gotten into a fight with. Marilyn was eager to win Sue's approval and fit into her group of friends, so she did as Sue requested.*

Cyberbullying and cyberthreats may be 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 becomes a cyberbully and retaliates online. Still other times, the student who is victimized will share his or her anger or depression online as distressing material. When school officials respond to a report of cyberbullying or a cyberthreat, it is exceptionally important to take the time to fully investigate the situation—through an analysis of online as well as Real World interactions. Students should be held accountable for harmful material posted online, but punishing the student who is being victimized at school for responding to this victimization online will only increase the potential for additional harmful acts.

> *Eric is frequently bullied at school, but rarely responds. His social networking profile contains many angry, and sometimes threatening, comments directed at the students who torment him at school.*

Cyberbullying may involve 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.

> *Annie has been going out with Jacob, but is starting to have second thoughts about their relationship. As she is trying to back off, Jacob has become more controlling. He repeatedly sends her text messages, demanding to know where she is and whom she is with.*

Cyberbullying may be based on hate or bias—bullying others because of race, religion, physical appearance (including obesity), or sexual orientation.

> *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.*

Teens may think that cyberbullying is entertaining—a game to hurt other people.

> *Sitting around the computer with her friends, Judy asked, "Who can we mess with?" Judy started IM-ing with Brittany, asking her many personal questions. The next day, the girls were passing around Brittany's IM at school.*

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 and avoidance, and, in some cases, school violence or suicide. It is possible that the harm caused by cyberbullying may be 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."
- Teens may be reluctant to tell adults what is happening online or through their cell phones because they are emotionally traumatized, think it is their fault, fear greater retribution, or fear online activities or cell phone use will be restricted.

> *A group of girls at Alan's school had been taunting him through instant messaging, teasing him about his small size, daring him to do things he couldn't do, suggesting that 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." This is also a true story.*

BULLY, TARGET, AND BYSTANDER

At this point in time, it is likely that many students who are actively socializing online, have had some involvement 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, or "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, who in some cases may be the bullies at school, and in other cases the targets.

- **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 against it, provide support to the target, or tell an adult. One of the most important strategies to address cyberbullying will be stimulating more students to become helpful bystanders.

RELATED ONLINE RISKY BEHAVIOR

Other concerns about online risky behavior that could be implicated in incidents of cyberbullying or cyberthreats include:

- **Disclosing Personal Information.** Young people are disclosing personal contact information and massive amounts of sensitive personal information in public online sites or through personal communications. Teens seem to be unaware of the public and permanent nature of these disclosures and the ability of others to send the material they place in electronic form to anyone, anywhere.

- **Internet Addiction.** Internet addiction is defined as an excessive amount of time spent using the Internet, resulting in lack of healthy engagement in other areas of life. The Internet offers a time-warped, 24/7 place where children and teens can get away from their real-world concerns.

- **Suicide and Self-harm Communities.** Depressed young people are interacting with sites and groups that provide information on suicide and self-harm methods (for example, cutting, anorexia, fainting) and encouragement for such activities.

- **Hate Group Recruitment and Gangs.** Sites and groups that foster hatred against "others" are actively recruiting angry, disconnected youth. Some youth informally use the Internet to coordinate troublesome and dangerous activities.

- **Risky Sexual Behavior.** Young people are using Internet communities and matching services to make connections with others for sexual activities, ranging from online discussions about sex to "hook-ups." They may post or provide sexually suggestive or explicit pictures or videos.

- **Violent Gaming.** Violent gaming frequently involves sexual or other bias-based aggression. Young people often engage in online simulation games, which reinforce the perception that all interactions online, including violent ones, are "just a game."

YOUTH RISK ONLINE FACTORS

Youth risk online must be viewed from perspective of adolescent risk. Young people are not equally at risk.

- **Savvy Teens**. Savvy teens have effective knowledge, skills, and values to make good decisions. They are likely to be older teens, with healthy peer relationships, and attentive parents who have fostered independence and personal responsibility.

- **Naïve Teens**. Naïve teens lack sufficient knowledge and skills to engage in effective decision-making. They are likely to be younger teens, have either over protective or naïve parents, but likely have healthy peer relations and good values—and with education can become savvy teens.

- **Vulnerable Teens.** Vulnerable teens lack the necessary knowledge and skills and are also are going through a period of "teen angst"—such as parental discord, difficulties in school, break-up of a relationship. They likely to have temporarily impaired relations with parents and/or peers and are currently highly emotionally upset.

- **At Risk Teens**. At risk teens are those who are "at risk" in other areas of life. These are the teens who face major ongoing challenges related to personal mental health and disruptions in relations with parents, school, and/or peers.

The higher the degree of risk, the greater the probability the young person will be:

- Searching for acceptance and attention from people online.

- More vulnerable to manipulative influence techniques used by dangerous individuals and groups.

- Functioning in "fight or flight" mode and thus less likely to make good choices because they are not "thinking clearly."

- Less attentive to Internet safety messages.

- Less resilient in getting out of a difficult situation even if he or she wants to.

- Less able or willing to rely on parents for assistance.

- Less likely to report an online dangerous situation to an adult because this will likely reveal evidence of their own unsafe or inappropriate choices.

Which means we must:

- Educate adults who are likely in the best position to detect and respond to concerns involving higher risk youth

- Develop effective teen "bystander strategies" to encourage teens to provide guidance and assistance to peers and report online concerns to adults

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? Here are some of the reasons:

- **You Can't See Me.** When people use the Internet, they perceive that they are invisible. The perception can be enhanced by creating anonymous accounts. People are not really invisible—online activities can be traced. But if you think you are invisible, this removes concerns about 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 these:

    - *"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 ignore or dismiss any online harm.

    - *"Look at me—I'm a star."* Supports excessive disclosure of intimate information and personal attacks on others, generally done for the purpose of attracting attention.

    - *"It's not me. It's my online persona."* Allows teens to deny responsibility for actions taken by one of their online identities.

    - *"What happens online stays online."* Supports the idea that one should not bring issues related to what has happened online into the outside 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.

LEGAL ISSUES

There are many legal issues related to cyberbullying and cyberthreats.

Search of Internet and Personal Digital Device Records

<u>When can a school monitor and search student Internet use records and files?</u>

The locker search standard should apply to student Internet use. Students have a limited expectation of privacy on the district's Internet system. Routine maintenance and monitoring, technically and by staff, should be expected. An individual search of computer and Internet use records can be conducted if there is reasonable suspicion that the student has violated district policy, including policies against bullying. Schools should determine who has authority to authorize individual search and record-keeping procedures. Clear notice to students can enhance deterrence.

<u>When can a school search electronic records on a student's personal digital device?</u>

There are some legal concerns related to conducting a search of a student's personal digital device, including cell phone, PDA, or personal laptop. Such a search may be a violation of wiretapping laws. (Additional guidance for how to address this concern will be provided on http://cyberbully.org by summer 2007.)

Free Speech

When can a school legally respond to cyberbullying by disciplining the student?

The First Amendment places restrictions on school officials when responding with formal disciplinary actions in situations involving online speech by students. Case law is limited.

The basic legal standard is that school officials can place educationally based restrictions on student speech that appears to be sponsored by the school or that is necessary to maintain an appropriate school climate. This standard probably applies to student speech through the district Internet system used at school.

For off-campus online speech or speech via personal digital devices used on campus, the courts have ruled that the speech must have caused or threaten to cause a substantial and material threat of disruption on campus or interference with the rights of students to be secure. But how this standard might be applied to severe off-campus, online speech by one student against another student is unknown.

The best way to handle the concern that the legal standards are unclear is to search diligently for, and document, a school "nexus" and to document the substantial and material harm that has been caused or is likely to be caused by the speech. A school "nexus may be found by demonstrating that harmful material was posted, sent or displayed to other students through district Internet system or on campus. If cyberbullying is closely connected to on-campus bullying, a school official may be able to address the cyberbullying in the context of the whole situation. If school "nexus" can't be found, it is safest to support victim in finding ways to resolve the situation. Contacting the parents of the cyberbully to seek informal resolution is likely the most effective response. The school resource officer may have more flexibility and influence in seeking an informal resolution.

Liability

When must a school respond to cyberbullying and cyberthreats?

District liability concerns are raised when cyberbullying or cyberthreats are occurring through district Internet system or when students are using personal digital devices while on campus. The parents of a victim may file a claim based on negligence or a civil rights violation, if the victim is a member of a protected class under state or federal law. Schools have a duty to exercise reasonable precautions against student cyberbullying through the district Internet system and via cell phones on campus. Although there is no case law in this area, reasonable precautions should include:

- Policy provisions that prohibit the use of the district Internet system and cell phones on campus to bully or harass other students.

- Education to students and staff about these policies.

- Effective supervision and monitoring of activities when using the district Internet system. (It is not possible to monitor use of personal digital devices.)

- A vehicle for students to report cyberbullying and cyberthreats confidentially or anonymously.

- An established procedure to respond to such reports.

Civil Litigation

When should parents of a target consider civil litigation against the bully and parents of the bully?

Civil laws provide the ability for cyberbully victims to sue the bully and the bully's parents to recover financial damages for injuries or require actions, such as removal of material and discontinuation of cyberbullying. Some cyberbullying activities meet the standards for what is called an intentional "tort" (wrongdoing).

In many jurisdictions, there are parental liability laws that allow someone who is intentionally injured by a minor to hold the parents of that minor financially responsible. Parents can also be found negligent in failing to provide reasonable supervision of their child. If a school official notifies parents that their child is cyberbullying another and the cyberbullying continues, this can provide an enhanced ability to hold the parent's financially liable. Informing the parents of the cyberbully about this potential is likely the strongest "motivation" school officials can use to ensure that the cyberbullying stops.

Depending on the facts, the following legal actions might be possible:

- **Defamation.** Someone publishes a false statement about a person that damages his or her reputation.

- **Invasion of privacy/public disclosure of a private fact.** Someone publicly discloses a private fact about a person under conditions that would be highly offensive to a reasonable person.

- **Invasion of personal privacy/false light.** Publicly disclosing information that places an individual in a false light.

- **Intentional infliction of emotional distress.** Someone's intentional actions are outrageous and intolerable and have caused extreme distress.

An attorney can send a letter to the bully's parents and seek informal resolution or file a lawsuit.

Criminal Law

When should a school contact, or assist a parent in contacting, law enforcement officials?

Extremely harmful online speech can violate criminal laws. The following kinds of speech can lead to arrest and prosecution:

- Making threats of violence to people or their property.

- Engaging in coercion (trying to force someone to do something he or she doesn't want to do).

- Making obscene or harassing telephone calls (this includes text messaging).

- Harassment or stalking.
- Hate or bias crimes.
- Creating or sending sexually explicit images of teens (this is child pornography).
- Sexual exploitation.
- Taking a photo of someone in place where privacy is expected (like a locker room)

COMPREHENSIVE SCHOOL AND COMMUNITY-BASED APPROACH

The following is a research-guided approach to address cyberbullying and cyberthreats based on: best practices in bullying, violence, and suicide prevention programs, research insight into bullying, violence and suicide, standard threat assessment and suicide intervention processes. This insight has been combined with: insight into online behavior of youth, analysis of legal issues, and an understanding of effective Internet use management practices in school and home.

This comprehensive approach is not yet research-based. If seeking to use federal safe schools funds to implement this program, a district must request waiver of Principles of Effectiveness. The necessary components to meet the waiver have been built into this approach.

Comprehensive Planning Through Safe Schools Committee

It is assumed that the district and schools have functioning safe schools committees. It is recommended that these committees that assume responsibility for addressing cyberbullying and cyberthreats. Safe school committees generally include: administrators and counselors/psychologists, and school resource officers. Hopefully, they also include community representatives including parents and mental health organizations.

In many districts, the safe schools committee has historically had no responsibility for issues related to management of student use of the Internet, including the district Internet use agreement. Such management is generally the responsibility of the educational technology committee. Frequently the safe schools committee and the educational technology committee function within two different district departments.

Addressing the concerns of cyberbullying and cyberthreats will require a systemic change. Most members of the safe school committee will have little understanding of how the district Internet system is managed and may have little insight into Internet technologies and activities. While some of the teacher or librarian members of the educational technology committee may have insight into safe schools issues, the technology staff may have much less insight. To manage the concerns of cyberbullying and cyberthreats, these two committees must work together, with the safe schools committee moving into a position of responsibility.

Ideally, the safe schools committee will also work closely with a group of students to address this concern. However, this is potentially problematical because these students could be viewed as traitors by their peers.

Needs Assessment—Bringing "Sunlight" to the Problem

A comprehensive student survey is necessary to identify the scope of the concerns in the district and to provide insight into underlying issues. The survey should address on-campus and off-campus instances, relationship to on-campus bullying, impacts, reporting concerns, and attitudes,

In addition to providing insight into the local concerns, the needs assessment survey results may be instrumental in bringing better awareness to the extent of the concerns, a prerequisite to bringing attention to the concerns.

The results of this survey, and other assessment instruments, can help to gauge success and provide insight into necessary modifications of the program and also meet the requirements for a waiver of the Principles of Effectiveness.

Policy and Practice Review

All policies and practices related to Internet use, use of personal digital devices while on campus, and bullying, violence, and suicide prevention processes for reporting, assessment, and intervention should be reviewed in the context of the concerns of cyberbullying and cyberthreats.

One specific new practice that is recommended is better notification to students during log-on to any district computer about policies against the use of district technology resources for bullying, the existence of monitoring and the right of the district to review individual student records, and an online confidential cyberbullying and cyberthreats reporting vehicle.

Professional Development

It is recommended that a "triage" approach be implemented to accomplish the necessary professional development. To address issues of in-school bullying, all staff require professional development. This is not the case with the concerns of cyberbullying and cyberthreats.

Several key people in the district (or region) need high level of expertise in the area of these concerns. Safe schools planning committee and all "first responders" (disciplinary administrators, counselors, school resource officers, librarians, and computer lab coordinators) need insight into problem and ways to detect, review, and intervene. These individuals will be able to gain necessary guidance on specific incidents from district level personnel. Teachers who are instructing students about cyberbullying need insight into the concerns and how to motivate safe and responsible behavior. All other staff likely require only general awareness.

Parent and Community Outreach

The school, as well as parent and community members, can help to facilitate parent and community outreach and education. Information should include an overview of the concerns, how to prevent, detect and intervene if children are a victims, preventing children from being cyberbullies, legal consequences, and strategies to empower and activate bystanders.

Information can be provided to parents through newsletters and parent workshops. Having "just-in-time" information resources available in office and online will be helpful because most parents are not likely to pay attention until they need the information to respond to a concern.

Information can also be provided to community mental health professionals, faith-based organizations, youth organizations, the public library and community technology centers and the media.

Student Education

While it is necessary to improve monitoring and apply consequences within a school environment (as well as encouraging parents to do this at home), it must be recognized that cyberbullying is occurring in online environments where there are no responsible adults present. Empowerment of youth to independently prevent and address these concerns is the goal of the student education.

The prerequisite to addressing cyberbullying is effective social skills education. Most schools are already providing this kind of education. Social skills instruction should enhance predictive empathy skills and teaching ethical decision-making and conflict resolution skills.

In addition, students need to have a better understanding of family, school, and legal limits on online speech, negative influences on online behavior, and Internet privacy protection. Students should be warned about the negative consequences of online retaliation and posting material that could be perceived as a threat. Students need specific guidelines on how to prevent and stop cyberbullying. Educating bystanders about the importance of speaking out, providing assistance to victims and reporting concerns is important.

Evaluation and Assessment

Implementing this approach using a “continuous improvement” approach is critically important. Cyberbullying is an emerging concern in a new environment that is not fully understood. Insight from emerging research will need to be incorporated. The needs assessment survey, as well as other assessment instruments, can help to assess program components. Evaluation and assessment should be used to modify and improve implementation efforts.

COMPREHENSIVE INTERNET USE MANAGEMENT

There is reason to suspect that cyberbullying behavior is occurring through district Internet systems. A local needs assessment will provide greater insight into this concern. It appears that districts or schools with laptop programs that allow the students to take the computers home are at a high risk for misuse.

Many districts are using filtering software as a primary means of seeking to manage student Internet use. Not only will filtering software not fully block access to inappropriate material, it is exceptionally difficult to use this as a tool to prevent cyberbullying. Essentially, it would be necessary to block or prevent all student use of the Internet for communications to do this. Such limitations would limit the educational value of the Internet.

A more comprehensive approach to managing student Internet use focuses strongly on protection for younger students by generally limiting their access to sites that have been reviewed for appropriateness and completely open and transparent communications. For older students, this strategy must focus on standards and effective technical monitoring to ensure

accountability. The key components of an effective approach to manage student Internet use include the following.

Focus on Educational Use

It is necessary to increase the level of use for high quality educational activities and decrease "Internet recess" activities. Educators know what happens during recess. This requires effective professional and curriculum development and specific expectations for teachers about the instructional use of technologies by students. The curriculum and instruction department should be responsible for coordinating educational technology-based instruction, not the technical services department.

Clear, Well-communicated Policy

The Internet use policy must be coordinated with disciplinary policies and address:

- Access to inappropriate material.
- Unacceptable communication and communication safety.
- Unlawful and inappropriate activities.
- Protection of student personal information.
- Notice of limited expectation of privacy.
- Requirement of reporting cyberbullying or threats.

Supervision and Monitoring

Effective supervision and monitoring is important for deterrence, detection, investigation, and responding to incidents of cyberbullying and cyberthreats. Monitoring should be sufficient to establish the expectation among students that there is a high probability that instances of misuse will be detected and result in disciplinary action. An effective supervision approach for teachers to us frequently and randomly request to see the browser history file of individual students whenever students are using the Internet in class.

Technical monitoring of district Internet use that utilizes intelligent content analysis is recommended as the best approach. This kind of a technology monitors all traffic and reports on traffic that has elements that raise a "reasonable suspicion," thus allowing an administrator to review such reports. The technology works in accord with "search and seizure" standards. Another technical approach to monitoring allows for real time remote viewing of any computer monitor in the building or computer lab.

Notice of the existence of monitoring will help to deter inappropriate activity. However it is important for students and staff to understand that no technology is perfect. Students should not to rely on monitoring, but should report any concerns.

CYBERBULLY SITUATION REVIEW AND ACTION OPTIONS

The attached documents provide guidance for school officials on the review and response to a report of an incident of cyberbullying or a cyberthreat.

Situation Review

School officials should establish a process to review situations involving cyberbullying incidents or cyberthreats. Review team members could include an administrator, counselor/psychologist, technology coordinator, librarian, school resource officer, and community mental health resource. However, for most incidents, this entire team will likely not be needed.

- **Imminent Threat.** If the online material appears to present a legitimate imminent threat of violence and danger to others school officials should contact law enforcement and initiate a protective response. But it is also necessary to continue with the following evidence gathering steps.

- **Evidence Gathering.** The evidence gathering should including preserving all evidence, and ensuring the identity of the cyberbully(ies), and may include searching for additional harmful material.

- **Violence or Suicide Assessment.** School officials should ask whether the evidence gathered raise concerns that student(s) may pose a risk of harm to others or self. Recognize that the threat of violence or suicide may come from student(s) who posted the material or from student(s) who were victimized.

- **Cyberbully Assessment.** An assessment must be made regarding whether the school can respond directly, with formal discipline by questioning whether there is a school nexus and substantial disruption or interference, or threat thereof. It is also necessary to gain a "root cause" understanding of the relationships and issues between the participants to determine whether harmful online material has been posted in retaliation for bullying.

Response Options

- **Formal Discipline.** School officials may be able to impose formal disciplinary response if a school nexus and substantial disruption has been established. But it is still necessary to address removal of materials, potential of continuation or retaliation by the student or online "buddies," and the support needs of the target.

- **Parent/Student/Staff Response Options.** Other response options, with or without formal discipline include:

    - Calmly and strongly tell the cyberbully to stop.

    - Ignore the cyberbully.

    - File a complaint with the web site, Internet service provider or cell phone company.

- Have the parents of the target contact the cyberbully's parents or contact an attorney.

- Contact the police.

About the Writer
Nancy 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 communication technologies. Willard frequently lectures and conducts workshops for educators on policies and practices to help young people engage in safe and responsible use of the Internet and has written numerous articles on this subject.

Center for Safe and Responsible Internet Use
The Center is a non-profit corporation that conducts research and provides resources and professional development to school districts to address issues related to the safe and responsible use of the Internet by students. Please visit the Center's web site at http://csrui.org for additional resources and information about professional development opportunities, including online workshops.

Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress **(Research Press)**
This document provides only a brief overview of the concerns. *Cyberbullying and Cyberthreats* provides extensive guidance for school officials on these concerns, with valuable implementation documents. More information at: http://www.researchpress.com/product/item/5306/

Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn to Use the Internet Safely and Responsibly **(Jossey-Bass)**
Cyberbullying and cyberthreats are just two of the concerns related to youth online behavior. Nancy Willard's new book, Cyber-Safe Kids, Cyber-Savvy Teens, provides extensive insight and guidance on all issues related to the safe and responsible use of the Internet by young people. More information at http://cyber-safe-kids.com.

> "Willard blends the perspectives of a wise parent and a serious scholar about issues related to Internet behavior and safety. . . . Pick up the book, open it to any random page, and you will find on that page or nearby a wealth of helpful advice and useful commentary on the cyberreality facing our children and on how to deal with any of the issues she's identified."
> —Dick Thornburgh, J.D., former U.S. Attorney General; chair, National Academy of Sciences Committee on Youth Pornography and the Internet