CENTER FOR SAFE AND RESPONSIBLE INTERNET USE

An Educator's Guide to Cyberbullying and Cyberthreats

Young people have fully embraced the Internet and other technologies, like cell phones, as both an environment and a tool for socializing. They send emails, create their own web sites, post intimate personal news in blogs (online interactive diaries), send text messages and images via cell phone, message each other through IMs (instant messages), chat in chatrooms, post to discussion boards, and seek out new friends in teen community sites.

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

This documents provides information about cyberbullying and cyberthreats for educators and other professionals who focus on youth safety and well-being and sets forth recommendations for a comprehensive school and community-based approach to address these concerns.

THE STORIES

These stories are based on actual events. Most names have been changed.

A group of girls at his school had been taunting Alan through IM, teasing him about his small size, daring him to do things he couldn't do. They dared him to commit suicide. He discussed this with them. The girls thought it was a big joke. One afternoon, Alan got his grandfather's shotgun, loaded it, and killed himself. He had deleted every thing from his computer, except for one message, "The only way to get the respect you deserve is to die."

The messages can get really outrageous on the student discussion board, especially when Nick is around. Nick thinks he knows everything. Anyone who dares to disagree with him or who posts what he thinks is a stupid comment is attacked with a vicious message.

Unknown middle school students created a web site all about Raymond. On this site, they posted Raymond stories, Raymond jokes, and Raymond cartoons. They posed questions about Raymond's sex life. They invited anyone visiting the site to submit their own comments and had an email link for people to send comments directly to Raymond.

Sitting around the computer with her friends at a Friday night sleepover, Judy asked, "Who don't we like? Who can we mess with?" They chose Sara, who was always trying to fit into the group. Sure enough, Sara was online. So Judy started IM-ing with her – with all of the other girls providing suggestions. "Ask her who she likes best, Jack or Nathan," they urged. The next Monday, the girls were passing 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, he sent it to classmates. Soon the picture was flying around to cell phones at school. By the time Greg left the locker room, all the students were laughing at him.

Joanne saw some girls bullying Jessica at school and reported the bullying to the office. By the time Joanne got home from school she had 35 angry messages in her email box and even more angry text-messages on her cell phone. Most of the messages are anonymous. Some appeared to be from strangers living in other parts of the country. Now, on a daily basis, Joanne gets many email and text messages using vulgar and insulting language.

Sara watched closely as Emma logged on to her school Internet account and was able to determine Emma's password. Later, Sara logged on to Emma's account and sent a scathingly cruel message to Emma's boyfriend, Alex.

An anonymous group of students from school have created a web site. The web site contains partially nude images of the girls, apparently taken in the girl's locker room. The web site offers visitors the opportunity to post comments about each girl. Many derogatory comments have been posted, including some that are sexually explicit.

When Annie broke up with her boyfriend, Sam, he sent her many angry, threatening, pleading messages. When Annie blocked his email account, Sam continued to send messages either by email or text message. When Annie still refused to get back with him, Sam posed as Annie in a sex-oriented discussion group and posted a sexually suggestive picture Annie had given him, along with her email address and cell phone number.

Jeff wrote the following comments in a series of chats: "I'm a retarded [expletive] for ever believing that things would change. I'm starting to regret sticking around, I should've taken the razor blade express last time around." "It takes courage to turn the gun on your ownself, takes courage to face death. Knowing you're going to die and actually following through takes heart, I don't care who you are.""... kind of rocky right now so I might disappear unexpectedly."

After he beat another boy in an online game, several of the boy's friends threatened Michael in the game site chat room. "We'll make you pay for this." Now when Michael tries to play on the site, a group of other players gang up on him and restrict his activities so that he cannot participate.

Celia met Andrew, a.k.a., nazi_bot_sadistic, in a chat room. As they continued to communicate, Celia became concerned. Andrew was obviously a very angry young man. He had no friends at school and expressed the desire to show the other students who he really was. Andrew wrote: "bring a gun to school, ur on the front of every newspaper … didnt choose this life, but i damn well chose to exit it … i cant imagine going through life without killing a few people … people can be kissing my shotgun straight out of doom … i tell it how it is .. if u dont like it u die … if i dont like the way u look at me, u die … i choose who lives and who dies"

CYBERBULLYING

Cyberbullying is being cruel to others by sending or posting harmful material using the Internet or a cell phone. Here is how it happens:

- Flaming. Online "fights" using electronic messages with angry and vulgar language.
- Harassment. Repeatedly sending offensive, rude, and insulting messages.
- 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.
- Denigration. "Dissing" someone online. Sending or posting cruel gossip or rumors about a person to damage his or her reputation or friendships.
- 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.
- Outing and Trickery. Sharing someone's secrets or embarrassing information online. Tricking someone into revealing secrets or embarrassing information, which is then shared online.
- Exclusion. Intentionally excluding someone from an online group, like a "buddy list" or a game"

CYBERTHREATS

A cyberthreat is online material that threatens or raises concerns about violence against others, suicide, or other self-harm. There are two kinds: Direct threats and distressing material

- Direct threats. Actual threats to hurt someone or commit suicide.
- Distressing Material. Online material that provides clues that the person is emotionally upset and may be considering hurting someone, hurting him or herself or committing suicide[1].

HOW

- 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 text/image cell phones. (See, Internet terms.)
- A cyberbully may be a person whom the target knows or an online stranger. A cyberbully may be anonymous and may solicit involvement of other people online who do not even know the target.
- Generally, teens are the most actively involved, sometimes children are. [We use the terms “teen” or “teenager” in this document.]

RELATED ONLINE RISKY BEHAVIOR

There are other concerns about youth online behavior related to the concerns of cyberbullying and cyberthreats. Teens who do not have strong “real world” connections appear to be the ones most attracted to these risky behaviors. These are the youth who are “looking for love in all the wrong places.”

[1] The stories of Alan, Jeff, and Andrew all demonstrate distressing material. Jeff was the student from Red Lake who killed nine people and himself. Celia saved and reported the chat. Andrew was found to be a member of a hate group and possess many weapons. He is now in prison.

Disclosing Personal Information

Young people are disclosing personal contact information and massive amounts of sensitive personal information in profiles, web pages, blogs, and through all forms of Internet communications. They seem to be totally unaware of the public and permanent nature of these disclosures and the ability of anyone to send whatever material they place in electronic form and send or post can be resent to anyone, anywhere in the world.

Internet Addiction

Internet addiction is defined as an excessive amount of time spent using the Internet, resulting in lack of healthy engagement in areas of life. Internet addiction is itself a concern, as well as an indicator of other concerns. The Internet offers a time-warped place where children and teens can get away from their real world concerns—they can be free, independent, uninhibited, and can find acceptance. The Internet is available 24/7. The game is always going on. Friends are always available. Life online constantly beckons.

One large part of the problem is that commercial web sites have designed “stickiness” into their operations—activities that are designed for the specific purpose of enticing young people to spend as much time as possible on their site and return frequently

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.” In the context of these relationships, they may post or provide sexually suggestive or explicit pictures or videos.

Suicide and Self-harm Communities

Depressed young people are interacting with sites and groups that provide information on suicide and self-harm methods and encouragement for such activities. Self-

harm includes cutting, anorexia, fainting, and the like.

Hate Group Recruitment and Gangs

Sites and groups that foster hatred against "others" are actively recruiting angry, disconnected youth. Some youth informally use Internet to coordinate troublesome and dangerous activities.

Violent Gaming

Violent gaming frequently involves sexual or biased-base victims. Young people often engage in online simulation games, which reinforce the perception that all interactions online, including violent ones, are "just a game."

Online Behavior

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?" The answer to this question can be summed up in one statement: "You can't see me, I can't see you."

You Can't See Me

When people use the Internet, they feel like they are invisible. It is just them, the keyboard, and the computer. In fact, people are not really invisible, because they are leaving little "cyberfootprints" wherever they go. The perception of invisibility is enhanced because of the ability to create anonymous accounts. When people are invisible, this removes the concerns of detection, social disapproval, and 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 else. The lack of tangible feedback interferes with empathy. This also leads to the perception that online actions are "just a game."

Rationalizations

Sometimes when people do something they know is wrong, they provide excuses or rationalizations for their behavior. Common rationalizations include: "He started it." "Everybody does it." "Nobody ever gets caught." "I was just playing around." It is a lot easier to rationalize wrong behavior online because of the perception of invisibility and the lack of tangible feedback.

Role Playing

Teens engage in role-playing online, by creating different "personas" or "avatars" in different online environments. This allows them to use a new Internet rationalization "It wasn't me. It was my 'avatar'." This reinforces the perception that all actions online are a game.

Online Social Norms

The perception of invisibility, lack of tangible feedback, and the ease by which wrong behavior can be rationalized, and role playing has provided the basis for online social norms that support for cyberbullying and cyberthreats. These norms include:

- "Tell all. On the Internet it is okay to reveal my personal secrets for the world to see."
- "I have a free speech right to say whatever I want about others online, without regard for the harm I might cause."
- "What happens online is just a game. It is not real. So no one can get really hurt."
- "What happens online, should stay online."

Why are educators (and parents) out of the loop?

Because in too many cases educators (and parents) aren't paying attention and teens aren't talking.

- Many educators think that if their students are using a computer in the library or a computer lab at school, they are safe and not getting into trouble. Nothing could be further from the truth.
- Educators may think students are protected because the district has installed filtering software. Filtering software pro-

vides false security. Not only can students still get to the kinds of material they should not access, it cannot prevent cyberbullying. Students could be the target of emotionally damaging harassment or be causing pain to others – using school computers. This is a special concern if the school has a lap-top program that allows the students to use computers from many locations, including home.

- There are strong social norms against disclosure of online concerns to any adult for fear of increased attention to online activities and restrictions and vicious retribution.

Bully, target, and bystander

Any student who has been actively socializing online, has probably been involved in cyberbullying in one or more of the following roles:

Bullies

- "Put-downers" who think they have the right to 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.

Targets.

- The target of the cyberbully. Some people call teens who are targeted by bullies "victims." We choose to use the term "target" because we do not believe that teens should ever be identified as "victims."

Bystanders

- Bystanders Who Are Part of the Problem. Those who encourage and support the bully or watch the bullying from the sidelines, but do nothing to intervene or help the target.
- Bystanders Who Are Part of the Solution. 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!

Insight into cyberbullying and cyberthreats

Bullying Behavior

- Bullying involves behavior intended to harm or disturb that occurs repeatedly over time among youth with an imbalance of power.
- Cyberbullying involves repeated behavior with intent to harm and repeated nature, but online communications can change power balance providing greater opportunity for a lower status target to retaliate.

Bullying Actions

- Bullying includes actions that are physical, direct verbal and indirect relationship aggression.
- There is no physical form of cyberbullying. Direct verbal forms include flaming, harassment, and cyberstalking. Indirect relationship aggression includes denigration, outing, trickery, impersonation, exclusion, and also cyberstalking.

Ages

- There is extensive bullying behavior in middle school, especially the first years, with decreased bullying in older grades.
- It appears that cyberbullying peaks in older grades.

Profiles

- Bully and victim profiles include aggressive bullies, social climber bullies, passive victims, bully/victims.
- Cyberbullying appears to frequently based on social climbing interactions. Sometimes, this involves students who would not normally be perceived by school officials as bullies. Targets of bullying are retaliating online.

Gender Differences

- It is frequently stated that "boys bully

more than girls." But this may be based on a failure to recognize socially harmful acts of girls as bullying. Boys engage in more physical bullying.

- It appears that girls are more active in cyberbullying. Cyberbullying is verbal, not physical. Girls are more involved in online communications, whereas boys play online games.

Sexual Harassment

- Sexual harassment is sometimes included in definition of bullying.
- There appears to be a significant amount of relationship-based cyberbullying, including failed relationships and relationship-based fights. Risky online sexual behavior can lead to failed relationships and the existence of sexually explicit images that can be used for cyberbullying.

Hate and bias

- Bullying can be motivated by hate and bias, based on gender orientation, obesity, race, and religion.
- Angry, disconnected youth are attracted to online hate groups or informal associations with other disaffected youth. Online games reinforce bias-based hate. Both of these factors appear to influence cyberbullying. Students who are obese or perceived to have a different sexual orientation are significant targets.

Bystanders

- Bystanders reinforce bullies and maintain social norms. Efforts to address bullying are focusing on empowering bystanders.
- There are no responsible adults in these online environments. Empowering online bystanders to disapprove, assist, and/or report will be essential to addressing the concerns of cyberbullying.

Parents

- Parents of bullies have been found to demonstrate lack of involvement, no limit setting, and model aggressive problem-solving.
- A frequent Internet use survey finding is that parents are not involved in their children's online activities. Promotion of filtering software has lead to false security and lack of parent monitoring.

Media Influences

- Some media glorifies bullying and violence and excessive personal disclosure.
- Teens can be star of their own "reality TV" show in their personal blog or web site by sharing personal information or slamming others. Online violence can be perceived as "just a game." Cyberbullying is a form of entertainment.

Impact

- 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."
  - Many teens are 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 their online activities or use of a cell phone will be restricted.

Cyberthreats – Direct Threats

- Youth make threats all of the time. Their

tone of voice, posture, overall circumstances allow others to determine whether or not the expression is a “real threat.”

- Threat communicated online could be real or NOT. Just because it is written and communicated electronically, does not make it “more real.” Online material that appears to be a threat could be:
  - Good-natured fun, a joke, nuisance activity, or a form of parody.
  - An online game or role-playing, where no part of the interaction is “real.”
  - Material posted by an anonymous individual impersonating another to get that person into trouble.
  - The last chapter in an ugly online fight, which has built to excessively harsh and threatening language, but with limited potential for any face-to-face violence.
  - A hormonal outburst that came and went.
  - A cry for help.
  - An imminent threat of violence to self or others.
  - Something else?
- School officials must be vigilantly cautious when responding to cyberthreats
- If a student is arrested for posting material that appears threatening, but is a joke, the most significant result will be that students will never again trust adults to respond appropriately and will not report subsequent possible threats.

Cyberthreats – Distressing Material

- “Leakage" or “suicide ideation” is considered to be one of the most important clues that may precede a violent act. Leakage occurs when a student intentionally or unintentionally reveals clues to feelings, thoughts, fantasies, attitudes, or intentions that may signal an impending violent act.
- Some teens have no one to talk with about how bad they are feeling and how horrible their life is. So they post material online that shares how hurt they are. They might think that if they post this kind of material online, they will meet someone who cares about them. Unfortunately, they may meet a dangerous stranger or hook up with other teens who reinforce their bad feelings.
- It should be assumed that emotional distraught youth with Internet access will likely post online material that provides significant insight into their mental state.
- Schools must learn how to find, analyze, and effectively respond to online “leakage” and specifically encourage youth to report this material.
- District threat assessment processes and suicide prevention processes MUST incorporate an analysis of the online postings of students.

Legal Issues

There are many legal issues related to cyberbullying and cyberthreats.

Search of Internet Records

When can a school monitor and search student Internet use records and files?

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.

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 and provides unclear guidance. 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 or via cell phones used at school. For off-campus online speech, the courts have ruled that there must be a substantial and material threat of disruption on campus. 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" to bring case under the educationally based restrictions standard and to document the substantial and material harm that has been 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 target in finding ways to resolve the situation or to contact the parents of the cyberbully to seek informal resolution. 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 via cell phone on campus. The parents of a target may file a claim based on negligence or a civil rights violation, if the target 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, which should likely include intelligent technical monitoring of Internet use.
- 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 consider civil litigation against the bully and parents of the bully?

Civil laws provide the ability for cyberbully targets 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. 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.
- 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. Parents may also file an action through small claims court, although this may require some sophistication.

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 the approach.

The recommended components of this comprehensive approach include the following components.

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, cell phone use 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.

The use or establishment of a student court to review cyberbullying concerns should be considered. Students are going to be far more receptive to the admonishment of other students on issues related to the use of new technologies. This may also be an effective way to handle incidents that could reach the level of a violation of a criminal law in lieu of processing through the juvenile justice system. An interesting area to explore would be the possibility of using a student court as a vehicle for a student target to bring what would be the equivalent of a civil law suit requesting injunctive relief (demanding actions but with no demand for financial damages).

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 require only general awareness.

Parent and Community Outreach and Education

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 targets, prevent-

ing 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 targets and reporting concerns is important.

Evaluation and Assessment

Ongoing evaluation is critically important. Cyberbullying is an emerging concern in a new environment that is not fully understood. 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

Anecdotal reports from schools reveal that there is reason to suspect that cyberbullying behavior is occurring through district Internet systems. The needs assessment survey will provide insight. 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. We all 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. Educational technology-based instruction should be coordinated by curriculum and instruction department, not the technical services department.

Clear, Well-communicated Policy

The Internet use policy be coordinated with other school disciplinary policies and should 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.

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. 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

Attached to this document is a chart that outlines an approach to manage the review of any reports of cyberbullying or cyberthreats.

School Action Options

The Situation Review will provide the background to determine possible actions options. These options include:

- Off-campus cyberbullying establishes a reasonable suspicion of wrong behavior, which should give the school the right to search the student's Internet use records, which could reveal evidence of a "school nexus."
- If the district can establish a school "nexus," and substantial interference with the target's ability to fully participate in school activities, the school can impose a formal disciplinary response.
- But do not simply impose a formal disciplinary response and expect the situation to be resolved. If a student has been victimized at school and is retaliating online, it is necessary to stop the on-campus bullying, as well as the online retaliation. Formal discipline could also trigger greater online retaliation against the target by the cyberbully and/or anonymous online "buddies." Get to the root of the problem!
- Parents will need to initiate some actions, see below. School officials can help the parents or the target figure out the most appropriate response(s) and provide a range of assistance in following through, including technical support.
- The school counselor or school security officer can seek an informal resolution with the parents of the cyberbully. The cyberbully's parents may be totally unaware, concerned to find that their child has engaged in this kind of activity, and get the cyberbullying to stop. Or they

could be very defensive. Send the cyberbully's parents a letter that includes the downloaded material and requests a meeting to address these concerns. It may be best to start with a school counselor initiated attempt at resolution and then shift to involving the school resource officer if the parents are not responsive.

- All staff should be informed about the cyberbullying and advised to report any negative incidents of in-school bullying between the participants, even very mild negative interactions.
- The school counselor should provide ongoing support to the target. The counseling support should address the harm and seek to empower the target with effective skills to prevent and respond to bullying, including...
  - Develop his or her personal guidelines for online involvement.
  - Make a realistic evaluation of the quality of the online community and the benefits of remaining in or leaving.
  - Recognize the need to leave an online situation that has gotten out of control.
  - Conduct a self-assessment of his or her behavior or communications that may be contributing to victimization.
  - Learn how to respond in an assertive, but not aggressive, way to any harmful communications.
  - Know when and how to gain assistance from an adult.

Parent, Student, Staff Action Options

Options for parent, student, or staff include:

Tell the Cyberbully to Stop

- The target could send a non-emotional, assertive message to the cyberbully telling him or her to stop.

Ignore the Cyberbully

- Block or filter all further communications through email and IM contact list.
- Avoid going to the site or group where he or she has been attacked.
- Change email address, account, username, or phone number.

File a Complaint

- Cyberbullying is a violation of the "Terms of Use" of most web sites, ISPs, and cell phone companies. File a complaint by providing the harmful messages or a link to the harmful material and ask that the account be terminated and any harmful material removed.
  - If the cyberbully is using email, contact the ISP of the cyberbully (determine the ISP from the email address), contact the company at <support@<ISP> or look on the ISP's site for a "Contact Us" email address.
  - If the material appears on a third-party web site (e.g. <http://www.webhostname.com/~kid's name.html>) go to site's home page, file a complaint through the "Contact Us" email address.
  - If the material is on a web site with its own domain name (e.g. http://www.xyzkid.com), go to Whois (http://www.whois.net) to find the owner of the site and the host company. Go to the host company's web site and file a complaint through the "Contact Us" email address.
  - If the cyberbully is using a cell phone, trace the number and contact the phone company.
  - Be sure to save the communications.
  - One problem is that the cyberbully can easily set up a new account. =

Contact the Cyberbully's Parents

- The target's parents can send the cyberbully's parents a letter that includes the downloaded material and requests that the cyberbullying stop and all harmful material be removed.

Contact an Attorney or File a Small Claims Action

- An attorney can send a letter to the cy-

berbully's parents demanding that the cyberbullying stop. An attorney can also help file a lawsuit or help the parents file a small claims action against the cyberbully's parents for financial damages and a requirement that the cyberbullying stop.

Contact the Police

- If the cyberbullying appears to be a crime, contact the police. Cyberbullying that involves threats of violence, coercion, obscene or harassing text messages, harassment or stalking, hate or bias crimes, creating or sending sexually explicit picture, sexual exploitation, or taking a picture of someone in private place could be a crime.

Internet Terms

- Profiles. Established on community sites generally during registration. Allow users to provide personal information and interests. Can be searched by other users.
- Username. A fake name that a user establishes during registration that identifies the user on that site. The username(s) that a teen selects can provide insight into the image or persona the teen seeks to establish in the particular community.
- Personal web sites. Sites to post material, including writings, drawings, and pictures. Generally more static. May allow users to comment.
- Blogs (weblogs). Interactive personal online diaries or journals. Teens share a significant amount of personal information in blogs. Others can submit comments.
- Email. Asynchronous (not real time) communication sent to individual(s) or a discussion list.
- Discussion groups or boards. Asynchronous group communications around a topic. Students often establish discuss groups that are school-related.
- Chat. Synchronous (real time) group communication, with ability to establish private chats.
- Instant messaging (IM). Synchronous private communications with anyone on a contact or "buddy list." Teens can have up to 450 "friends" on their "buddy list."
- Text/digital image messaging. Messages or images sent via cell-phones.
- Gaming. Online interactive games that are played user against the machine or that involve two or more users. Some gaming sites include extensive ongoing simulation activities where the gamer assumes a permanent character (persona or avatar) whenever he or she is involved in the gaming site. Many games involve violence, sometimes sexual or biased-based violence.
- Social networking communities. Web sites that combine the features of profiles, personal web sites, blogs, discussion groups/boards, chat, gaming, and messaging. All the rage with teens! Look at http://www.myspace.com, http://www.bolt.com, http://studentcenter.org, http://www.livejournal.com.
- Important insights about online environments: Web site or provider Terms of Use generally prohibit harmful speech, but do not review postings. Concerns must be reported to the site. Many sites have age limits older than 13 or 16, but youth know they can easily lie about their age during registration.

About the Writer

Nancy Willard, M.S., J.D. 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 conducts research and provides resources and professional development to school districts and others. Please visit the Center's web sites at http://cyberbully.org or http://csriu.org for additional resources.

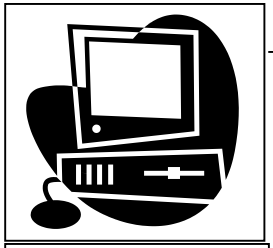
Cyberbullying and Cyberthreats Part I: A Guide for Counselors, Teachers and Parent Educators Available December 2005. Part I contains a reproducible Teen's Guide (student curriculum) and Parent's Guide. *Part II: A Comprehensive School, Parent, and Community Approach* will be available Summer 2006.

Cyberbullying or Cyberthreat Situation Review Process

Review Team Members

- Administrator
- School counselor or psychologist
- Technology coordinator
- Librarian
- School resource officer
- Community mental health resource
- Key district/regional resource

Entire team may not be needed in all cases.



Online Incident

If the online material appears to present a legitimate imminent threat of violence and danger to others, contact law enforcement, and initiate a protective response.

BUT continue with the following evidence gathering and preservation steps.

Evidence Gathering and Preservation

Step 1. Preserve the Evidence
- Preserve any evidence on district Internet system.
- Advise parents/student/staff to preserve evidence on home computer/device.
  - Offer technical assistance, if necessary.

Step 2. Seek to Identify Creator(s)
Responsibility: Technology coordinator.
- May be obvious, anonymous, or impersonation.
- Identification may not be immediately possible.
- Offer technical assistance to parents/staff.
- If anonymous cyberbully or concerns of impersonation, and there are reasons to suspect certain student(s), conduct a search of Internet use records of student(s).
- If criminal action is involved, law enforcement has significantly greater abilities to identify anonymous creators.

Step 3. Search for Additional Material
Responsibility: Technology Coordinator and Librarian.
- Search should include all suspected participants.
- Conduct search of files and Internet use records through district Internet system (even if it appears to be off-campus activity).
- Conduct an additional search including
  - Online environment where initial material appeared.
  - Search engine search for name and persona of student, friends, enemies, school name.
  - Online communities used by students in school.

Highly recommend this step be taken in the context of **any** threat assessment process!

Center for Safe and Responsible Internet Use
Website: http://cyberbully.org and http://csriu.org
Email: info@csriu.org

Violence or Suicide Risk Assessment

- Does 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.

→ Conduct violence or suicide risk assessment in accord with district process.

Cyberbullying Assessment

Step 1. Determine if School Can Respond Directly
- Is there a school "nexus?"
- Is there a material and substantial threat of disruption?

Step 2a. Evaluate speech directed at staff or school
Determine the nature of the material.
- Nuisance activity → Ignore it.
- Legitimate protest speech → Fully protected speech. Learn from it.
- "Put down" material, targeting teacher for perceived "negative" feature → If school nexus, respond. If no school nexus, support teacher in responding.
- "Get back at" material, angry retaliation against teacher → Must determine why student is retaliating and address overall concerns.

Step 2b. Evaluate material directed at student(s)
Must get to "root cause" understanding of relationship between students.
- "Put down" material → Possible continuation of in-school bullying.
- "Get back at" material → Possible retaliation for in-school bullying or other cyberbullying.

Determine Response Options
(See page 2)

School and Parent Action Options

School "Nexus"
If there is a school "nexus" and substantial harm, the school can impose formal discipline.

- But do not simply impose a formal disciplinary response and expect the situation to be resolved. Get to the root!
- Other actions by the school or by the parent, target, or staff member may be necessary.

No School "Nexus"
If there is no school "nexus," provide support to the target and parents, and seek an informal resolution with cyberbully and parents.

- School officials can help the parents or the target figure out the most appropriate response(s) and provide a range of assistance in following through, including technical support.
- The school counselor or school security officer can seek an informal resolution with the parents of the cyberbully. The cyberbully's parents may be totally unaware, concerned to find that their child has engaged in this kind of activity, and get the cyberbullying to stop. Or they could be very defensive. Send the cyberbully's parents a letter that includes the downloaded material and requests a meeting to address these concerns. It may be best to start with a school counselor initiated attempt at resolution and then shift to involving the school resource officer if the parents are not responsive.
- All staff should be informed about the cyberbullying and advised to report any negative incidents of in-school bullying between the participants, even very mild negative interactions, because this can establish a school nexus.
- School counselor should provide ongoing support to the target. The counseling support should address the harm and seek to empower the target with effective skills to prevent and respond to bullying, including...
  - Develop his or her personal guidelines for online involvement.
  - Make a realistic evaluation of the quality of the online community and the benefits of remaining in or leaving.
  - Recognize the need to leave an online situation that has gotten out of control.
  - Conduct a self-assessment of his or her behavior or communications that may be contributing to victimization.
  - Learn how to respond in an assertive, but not aggressive, way to any harmful communications.
  - Know when and how to gain assistance from an adult.

Parent, Target, or Staff Member Action Options

Tell the Cyberbully to Stop

- Send the cyberbully a non-emotional, assertive message telling the cyberbully to stop.

Ignore the Cyberbully

- Block or filter all further communications through email and IM contact list.
- Avoid going to the site or group where the attacks have occurred.
- Change email address, account, username, or phone number.

File a Complaint
Cyberbullying is a violation of the "Terms of Use" of most web sites, ISPs, and cell phone companies. File a complaint by providing the harmful messages or a link to the harmful material and ask that the account be terminated and any harmful material removed.

- If the cyberbully is using email, contact the ISP of the cyberbully (determine the ISP from the email address), contact the company at <support@<ISP> or look on the ISP's site for a "Contact Us" email address.
- If the material appears on a third-party web site (e.g. <http://www.webhostname.com/~kid'sname.html>) go to site's home page, file a complaint through the "Contact Us" email address.
- If the material is on a web site with its own domain name (e.g. http://www.xyzkid.com), go to Whois (http://www.whois.net) to find the owner of the site and the host company. Go to the host company's web site and file a complaint through the "Contact Us" email address.
- If the cyberbully is using a cell phone, trace the number and contact the phone company.

Be sure to save all of the communications.
One problem is the cyberbully can set up a new account.

Contact the Cyberbully's Parents
The target's parents can send the cyberbully's parents a letter that includes the downloaded material and requests that the cyberbullying stop and all harmful material be removed.

Contact an Attorney or File a Small Claims Action
An attorney can send a letter to the cyberbully's parents demanding that the cyberbullying stop. An attorney can also help file a lawsuit or help the parents file a small claims action against the cyberbully's parents for financial damages and a requirement that the cyberbullying stop.

Contact the Police
If the cyberbullying appears to be a crime, contact the police. Cyberbullying that involves threats of violence, coercion, obscene or harassing text messages, harassment or stalking, hate or bias crimes, creating or sending sexually explicit picture, sexual exploitation, or taking a picture of someone in private place could be a crime.