An Educator's Guide to Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Use of the Internet
Web sites: http://csriu.org and http://cyberbully.org
E-mail: nwillard@csriu.org

December 2006
This material is a brief overview of these concerns.
Please refer to *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress* (Research Press)

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 social networking sites.

Unfortunately, there are increasing reports of teens, and occasionally younger children, using these technologies to post cruel text or images to bully their peers or engage in other aggressive online 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 document 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.

Cyberbullying

There are different forms of cyberbullying, which could also be called "online social aggression." These include:

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

  Joe and Alec's online fight got angrier and angrier. Insults were flying. Joe 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 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 damage that person's reputation or friendships.

  Laura watched closely as Emma logged on to her account and discovered her password. Later, Laura logged on to Emma's account and sent a scathing message to Emma's boyfriend, Adam.

- Outing. 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. Tricking 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 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 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 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."

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

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.

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 "lock-down." Greg was identified easily—and arrested for making a threat.

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.”

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.

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.

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.

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

There appear to be a number of factors are influencing teens to engage in harmful online behavior. These factors are normal teen development issues that are impacted by the use of technology.

Brain Development

Teens are in process of developing frontal lobes that allow for reasoned and ethical decision-making. Learning to make reasoned and ethical decisions requires attention to the connection

between actions and consequences. Use of technologies can interfere with the recognition of the connection between an action and a harmful consequence.

Online Disinhibition

People tend to do things online that they would not normally do in Real Life. Researchers call this "online disinhibition." There appear to be two principal factors that underlie this behavior:

- You can't see me. The perception of invisibility and ability to create anonymity can remove concerns of detection and resulting disapproval or punishment.
- I can't see you. The lack of tangible feedback of the impact of online actions interferes with recognition of harm caused, and resulting empathy and remorse.

Teen Emotional and Social Development

Teens are going through a period of intense emotional and social development. This includes exploration and establishment of their personal identity and emerging sexuality, as well as their social status and relations with others. Social networking profiles become a vehicle for teens to present their emerging self-image, which can their thoughts about others in their social environment. Teens are using social networking as vehicle to establish their "place" within their social community. A high number of friendship links and communication activity is perceived to reflect a high social status. Social status issues underlie much of in-school, as well as online, bullying behavior.

"At Risk" Youth

Youth who are "at risk" generally are highly vulnerable online. They may become involved with dangerous individuals or groups where they find acceptance and reinforcement for unsafe attitudes and behavior. "At risk" youth generally have lower levels of resilience in the face of online aggression, and thus may respond to such aggression in a manner that escalates the situation in potentially dangerous ways.

Online Social Norms

Because the disinhibition factors are impacting all online users, online social norms have emerged that support certain kinds of behaviors as "appropriate." Some common online social norms that support aggressive online behavior include:

- "Everyone does it."
- "If I can do it, it must be okay"
- "Life online is all just a game."

Free Speech Norm

One particularly concerning online social norm is: "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." Internet civil liberties organizations strongly support this norm. But just as it is not acceptable to shout "fire" in a movie theater, there are limits on free speech rights. These limits are grounded in:

- Personal values.
- Family and spiritual values.
- School rules.
- Terms of use agreements of Internet service providers, web sites, and cell phone companies.
- Civil law standards.

  - Defamation.
  - Invasion of privacy by disclosure of private fact or placing someone in false light.
  - Intentional infliction of emotional distress.
- Criminal law.
  - Threats of violence.
  - Harassment or stalking.
  - Hate or bias crimes.
  - Material harmful to minors, child pornography, or sexual exploitation.
  -

A very helpful learning exercise for students is to investigate the standards for how others should be treated that are embodied in all of these sources and note the similarities. There is a not-so-amazing concurrence of common values.

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.

Not Paying Attention

Educators and parents may think young people are protected online because of filtering software. Filtering software provides 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. Or conflict may be instigated when students are using the Internet at home and then come to school

Students are also using cell phones and other personal digital devices for such harmful activities, in school and out of school.

Not Talking

Teens are very reticent to disclose any online concerns to any adult. There are several reasons for this fear:

- Teens recognize that adults are overly fearful of Internet technologies and, as a result, will overreact.
  - One probable overreaction is increased online restrictions – essentially requiring the targeted teen to leave the harmful online environment or cutting that teen off from Internet activity. For today's teen, such a response is the equivalent of self-excommunication.
- Teens also fear that adults will not know how to respond effectively and that whatever they do will only exacerbate the harm. Online retaliation can be vicious.
- Many teens think that harmful online communications are the accepted social norm and they should simply "deal with it."

How, Where, Who, Why

There is insufficient high quality academic research of these concerns to draw any strong conclusions about these concerns. All of the following insights are based on observation, anecdotal reports, and some preliminary research.

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 cell phones. Much of this harmful activity is now occurring on social networking sites. Social networking sites allow teens to express their personal identity and maintain electronic connections with friends. Teens create profiles and blogs to share their interests and thoughts, establish friendship links, and engage in public or private discussions. There are many positive aspects of social networking, but these sites can be used aggressively against others.

These sites and services have terms of use that prohibit posting harmful material and will respond by removing such harmful content and may also terminate the membership of the offending poster. But educators, parents, and students must know how to file a complaint.

Off-campus/On-campus

A significant amount of cyberbullying is occurring off-campus but is impacting student relationships on-campus. It is also likely that students are using the district Internet system, cell phones, and other digital devices at school to engage in cyberbullying.

Who is It?

It may be quite easy to identify the cyberbully based on names provided, the address from which the material has been sent, or the site upon which the material is posted. Some instances may involve cyberbullying-by-proxy – where the bully solicits involvement of other people who may not even know the target. Other incidents may involve an anonymous cyberbully. Or a cyberbully may impersonate another for the purpose of getting that person in trouble.

Generally, teens are not very good at hiding their identity and a skillful investigation will result in an accurate identification. School officials should review all material posted for clues. If the material has been posted on a social networking profile, the friendship links can provide excellent insight. Generally it is easy to identify students through the material associated with these links. Once identified, interviews with less-involved students can result in an identification of the major aggressor(s). Law enforcement officials have greater ability to obtain identity information through the subpoena process.

Relation to School Bullying

Cyberbullying may be a continuation of in-school bullying or may be in retaliation for in-school bullying. Harm inflicted at school may result in the targeted student posting threats or distressing material online. School officials MUST NOT immediately assume that the student posting the harmful online material is the originator of the problem. It is essential to get to the root of the problem and not simply apply inappropriate punishment to the student who is being harmed at school.

School officials should closely evaluate the “social status” level of all of the participants. If a student who has posted harmful online material is at a lower social status level than the individual(s) targeted, it is probable that this material is posted in retaliation for bullying or other harm inflicted at school. Interviews with the students about other school interactions and discussions with staff about the relationships between the students can also provide insight.

Social Status Bullying

It appears that students most often involved in cyberbullying are the “in-crowd” students. “Wannabes” appear to be the most frequent targets. These are the students who are most actively interacting with each other in online environments. This assessment is not in accord with typical “bully” (mean kid) profile. Students who are engaged in cyberbullying are frequently

not perceived to be bullies at school. It is possible that the analysis of cyberbullying incidents will provide greater insight into bullying behavior at school.

Losers and Outcasts

Students who are identified as “losers” or “outcasts” at school appear to be less inclined to participate actively in the online social dynamics of members of the school community. These students may be targets of indirect cyberbullying. They may be posting angry condemnations of the students and staff who denigrate them at school on their own sites. They may also form their own online troublesome groups or participate in unsafe or dangerous communities. This involvement could have very dangerous consequences.

Boys or Girls

It is frequently stated, “boys bully more than girls.” But this may be based on a failure to recognize socially harmful acts of girls as bullying. There is some evidence that girls are more actively engaged in cyberbullying than boys. Girls tend to be more actively involved in online communications, which is the venue for cyberbullying. Boys tend to be interested in gaming, which involves violence against fictional characters.

Personal and Sexual Relationships

There appears to be a significant amount of relationship-based cyberbullying – including failed relationships and relationship-based fights. Risky online sexual behavior can also result in the existence of sexually explicit images that are used for cyberbullying.

Hate or 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 that reinforce hateful attitudes, which can lead to hate-based communications. Some online games also 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 frequently targets. Cyberbullying based on sexual orientation been implicated or suggested in many of the cyberbullying cases that have resulted in suicide.

Online Role-Playing Games

For some teens, cyberbullying or cyberthreats activity may be related to involvement in online role-playing gaming. Online role-playing games involve small groups of players in the development and execution of plans for a violent attack within the simulated game environment. There has been a recent reported phenomenon of groups of boys planning violent school attacks online. News reports indicated that these boys were considered “outcasts” at school and were actively involved in online gaming. Although clearly not yet demonstrated by research, this is a concern that school officials should be attentive to.

Roles

There appear to be two kinds of bullies: “Put-downers” who harass and demean others they think are different or inferior. “Get-backers” who have been bullied by others at school and are using the Internet to retaliate or vent their anger. Therefore, there are also two kinds of targets. Those who are also bullies at school, and those who are the bullies at school. It is essential that school officials recognize that use of Internet technologies has impacted the power status of students and seek to get to the root of the situation regarding the relationships between the students.

There are also two kinds of bystanders: Harmful bystanders encourage and support the bully or watch the bullying from the sidelines, but do nothing to intervene or help the target. Helpful

bystanders seek to stop the bullying, protest it, provide support to the target, or tell an adult Educating and empowering helpful bystanders is a critically important prevention and intervention strategy.

Targeting Staff

Students are also posting harmful material targeting teachers or other staff. This material could be a range of types:

- Staff person is targeted for denigration because of some perceived social status issue, such as sexual orientation or obesity.
- Student retaliation because he or she has been bullied or mistreated by the teacher.
- Youthful outburst, a convenient target, and a lack of sensitivity to the harm caused.
- Legitimate objections to the actions or policies of the school or staff.

Impact of Cyberbullying

It is possible that the harm caused by cyberbullying may be greater than 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" so the target may not know whom to trust.
- Teens may be reluctant to tell adults what is happening online or through their cell phone because they are emotionally traumatized, think it is their fault, fear greater retribution, or fear online activities or cell phone use will be restricted.
- There are reports of cyberbullying leading to suicide, school violence (including one school murder), school failure, and school avoidance.

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." A threat that is 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:

- 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.

School officials must be vigilantly cautious when responding to cyberthreats. Continuous reassessment must occur. The ultimate resolution must be in accord with the actual degree of threat – not the initial assessment.

There are two messages that are very important to communicate to students:

- Don't post material that an adult might perceive to be a threat.
- Report any material that appears to be a threat, because it is better to risk a report that turns out to be false than real harm if the threat is real.

Schools should use "teachable moments," such as news stories from other communities or events that happen within the district, to communicate these messages to students.

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. Schools should assume that many emotional distraught youth with Internet access will post material online that provides insight into their mental state and the reasons for that mental state. Threat assessment protocols and suicide prevention plans MUST be revised to incorporate the reality that significant amount of teen communication related to threats and suicide will be occurring online! Schools must learn how to find, analyze, and effectively respond to online "leakage" and specifically encourage youth to report this material.

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.

What about cell phones or other personal digital devices—laptops, PDAs, digital cameras—used by students on campus?

There is a significant legal concern about reviewing such records. It is likely that such review would be considered a violation of wiretapping laws. It is probable that districts will need to address this issue by contract that all parents must sign if they want their child to be allowed to use any personal digital device in school. If students use these devices in the classroom for instructional activities, staff must have the right to supervise their use in similar manner to the use of district technologies. If there is a reasonable suspicion that a user has violated district

policy or the law with one of these devices, school officials should have the right to review the stored records. The contract will likely need to include a provision for retention of the device, notice, and a right to appeal.

Free Speech

When can a school legally respond to cyberbullying with formal discipline?

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 online speech posted when the student is off-campus, 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 and there is not a significant threat of harm, 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 a personal digital device 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 personal digital devices 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 personal digital devices 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. Communicating to parents of a student who has engaged in aggressive online behavior that they could be held financially liable for harm caused by their child can be very helpful in supporting a strong parental commitment to ensure such online harm ceases.

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 U.S. federal safe schools funds to implement this program, a district must request waiver of Principles of

Effectiveness. The necessary components to obtain the waiver have been built into the 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 community 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 may be 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 and personal digital device use on campus, and violence and suicide prevention processes for reporting, assessment, and intervention should be reviewed in the context of the concerns of cyberbullying and cyberthreats. Internet use management practices are discussed below.

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.

It is essential that an anonymous/confidential process to file reports of online concerns be established and that a process for effective review and response occur.

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

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, 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 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 or Cyberthreat Situation Review

The attached document provides an overview of the review steps and action options that schools can take to address specific incidents.

Cyberbullying or Cyberthreat Situation Review Process

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 steps.

Review Team Members

- Administrator
- Counselor/psychologist
- Technology coordinator
- Librarian
- Resource officer
- Community mental health
- Key regional resource

Entire team may not be needed.

Evidence Gathering

Step 1. Preserve the Evidence
- Preserve all evidence from district Internet system.
- Advise parents/student/staff to preserve evidence on home computer. Offer technical assistance.

Step 2. Seek to Identify Creator(s)
- May be obvious, anonymous, or impersonation. Identification may not be immediately possible.
- Offer technical assistance to parents/staff.
- If anonymous or concerns of impersonation, and reasons to suspect certain student(s), conduct a search of Internet use records of student(s).
- If criminal action, contact law enforcement.

Step 3. Search for Additional Material
- All suspected participants.
- Search all files and Internet use records through district system (even if it appears to be off-campus activity).
- Conduct additional search including:
  - Site where initial material appeared.
  - Search engine search for name and username(s) 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! Search for additional material may lead to evidence of legitimate, imminent threat.

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.

Cyberbullying Assessment

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

Step 2A. Evaluate material directed at student(s)

Must get to "root cause" understanding of the relationships and issues.
- "Put down" material → Continuation of in-school bullying.
- "Get back at" material → Retaliation for in-school bullying or other cyberbullying.

Step 2B. Evaluate material directed at staff or school

Determine the nature of the material.
- Nuisance activity → Ignore it or seek to have it removed.
- 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 → Remove speech, but must determine why student is retaliating and address underlying concerns.

School Actions and Options

Formal Disciplinary Action
Can impose formal disciplinary response if have established a school nexus and substantial and material disruption. But still need to address:
- Removal of materials and potential of retaliation by student or online "buddies."
- If "put down" cyberbully stop all in-school bullying. If "get back at" cyberbully, stop al in-school victimization.
- Support needs of target.

If cannot impose formal discipline, other action options still available.

Working With Parents

Child who is "Put Down" Cyberbully
Assumptions
- Parents unaware, but actions are against family values.
- Initial response will be disbelief, followed by anger and humiliation.
- Parents naïve about strategies to manage Internet use.

Process
- Send downloaded material and *Parent's Guide* to parents via certified mail.
- Request meeting following day.
- Seek parental commitment to:
  - Establish prohibitions.
  - Prevent retaliation.
  - Install and use monitoring software.
  - Limit student's access through other venues.

Increased potential for financial liability through civil litigation is a strong leverage.

Child who is Target, "Get Back At" Cyberbully, or Who Has Posted Distressing Material
- Parent could approach school or school could find out from other source.
- Initial response of parents will be significant concern for safety and well-being of child.
- If contacting parent about reported concern, establish preliminary plan of action for support prior to meeting with parents.
- If working with parent of "get back at" cyberbully or student who has posted distressing material:
  - Ensure material is removed.
  - Install and use monitoring software.
  - Address underlying bullying or emotional concerns.
- If working with parents of target:
  - Explain limitations on formal response.
  - Use appropriate Response Options to stop/remove harmful material.
  - Warn to watch for retaliation.

Working with Students

Working with Student Who is Target
Addiction
- Address concerns of addiction to harmful online community.
  - Convince target to leave community.
  - Find way to get the cyberbullying to stop within the community.

Online Bully-Proofing
- Communications are preserved, so student and counselor can evaluate and determine patterns of communication that may be precipitating bullying.
- Impact of harmful communication is invisible if target does not immediately respond.
- Delay in communications can provide opportunity for target to calm down and respond with strength.

When to Ask for Help
Encourage students to tell an adult if:
- They are really upset and not sure what to do.
- The cyberbullying could be a crime.
- Any cyberbullying is or might be through the Internet of cell phone at school.
- They are being bullied by the same person at school.
- The cyberbully is anonymous.
- The cyberbully is bullying other teens who may be more vulnerable.

Parent/Student/Staff Response Options
- Challenge the cyberbully to stop.
- Ignore the cyberbully.
- File a complaint.
- Have the parents contact the cyberbully's parents.
- Contact an attorney.
- Contact the police.

Center for Safe and Responsible Internet Use
http://cyberbully.org