Cyberbullying and Cyberthreats
Effectively Managing Internet Use Risks in Schools

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
© 2006, 07 Nancy Willard
Permission to reproduce and distribute
for non-profit, educational purposes is granted.
January 2007

Safe Kids ~ Savvy Teens

- The Cyber-Safe Kids, Cyber-Savvy Teens "Formula."
  - When children are young, they should only use the Internet in safe places and we must teach them simple safety rules.
  - But as they grow and become teens, we must provide them with the knowledge, skills, and values to independently make good choices online.
  - And remain "hands-on" to ensure they do.

Cyberbullying

- Cyberbullying is being cruel to others by sending or posting harmful material or engaging in other forms of social cruelty using the Internet or other digital technologies.
- Online social aggression.

Different Forms

- Flaming.
  - Online "fights" using electronic messages with angry and vulgar language.
- Harassment.
  - Repeatedly sending offensive, rude, and insulting messages.
- 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 or images 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.”
- 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.

Cyberthreats

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

Other Significant Risks

- Sexually Related Risks.
- Unsafe Communities.
- Dangerous Groups.

Sexually Related Risks

- Pornography.
  - Accidentally accessing online pornography.
  - Intentionally accessing pornography in an addictive manner.
- Sexual Activity.
  - Being groomed by adult predators to engage in sexual activities or provide pornography.
  - Seeking sexual “hook-ups” with adults or other teens.
- Sexual Harassment.
  - Being victimized by or engaging in sexual harassment.
- Displaying Sexual Exploits.
  - Posting or sending sexually provocative or explicit images.
  - Discussing sexual exploits publicly.

Unsafe Online Communities

- Depressed teens becoming involved in “its-your-choice” self-harm communities.
  - Suicide.
  - Cutting.
  - Anorexia.
  - Passing out.
- Find acceptance from like-minded peers.
- Leads to contagion of unhealthy attitudes and behavior.

Dangerous Online Groups

- Angry teens becoming involved in hate groups or gangs with adult members and recruiters.
- Or forming their own troublesome youth groups.

- Find acceptance from like-minded peers or adults.
- Leads to contagion of unhealthy attitudes and behavior.

Foundational Concerns

- Safe or Unsafe Provision of Personal Information.
- Addictive Access and Media-Multitasking.
- Stranger Literacy.

Unsafe Personal Disclosure

- Many teens appear to have limited understanding of potential harm or damage from inappropriate information disclosure.
  - But are highly sensitive to any intrusion by parents or other responsible adults.
- Simplistic rule - “Do not disclose personal information online” - is insufficient.

Addictive Access

- Addictive access is an excessive amount of time spent using the Internet resulting in lack of healthy engagement in other areas of life.
  - Social networking addiction.
    - Social anxiety over acceptance and status.
  - Gaming addiction.
    - Addictive features of the gaming environments.
    - Lack of healthy peer connections.

Online Strangers

- Teens will have increasing engagement with online strangers.
- Sometimes teens will want to meet in-person with an online stranger.
- Most strangers are safe, but some are not.
- Learning to assess the safety of someone met online and knowing how to arrange for a safe meeting is an essential new safety skill.

Not-so-good Choices

- Why are some teens making not-so-good choices?
  - Brain development.
  - Disinhibition.
  - Exploration of identity.
  - Online social norms.
  - Social influence used to manipulate.

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.

Disinhibition

- Use of technologies interferes with recognition of connection between action and consequences.
- You can't see me.
  - Perception of invisibility, creation of anonymity removes concerns of detection and resulting disapproval or punishment.
- I can't see you.
  - Lack of tangible feedback of impact of online actions interferes with recognition of harm caused, and resulting empathy and remorse.

Exploration of Identity

- Social networking profile becomes vehicle to present emerging self-image.
  - Which includes emerging sexuality.
- Social status games.
  - Teens are using social networking as vehicle to establish their "place" within their social community.

Online Social Norms

- "Everybody does it."
- "Life online is just a game."
- "It's not me—it's my online persona."
- "What happens online, stays online."
- "I have the free speech right to write or post anything I want regardless of the harm it might cause to another."
- "If I can do it, it must be okay."

Social Manipulation

- Individuals and groups use manipulative social influence techniques online.
  - Provide a gift (tangible or intangible), which creates a feeling of indebtedness.
  - Obtain a commitment to certain attitudes and behaviors.
  - Go along with what the group thinks or does.
  - Comply with requests from people who are known and liked.
  - Respect and obey people in a position of authority
  - Act now or you will lose.

Cyberbullying Insight

- How.
- Where.
- Who.
- Relation to school bullying.
- Social status issues.
- Boys or girls.

- Personal relationship issues.
- Hate or bias.
- Roles.
- Impact.

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.
- Sites and services have terms of use that prohibit posting harmful material.
  - Will respond by removing such harmful content and terminating the membership of the offending poster.
  - But educators, parents, and students must file a complaint.

Where

- Significant amount occurring off-campus.
  - But is impacting student relationships on-campus.
- It is highly likely students are using the district Internet system or personal cell phones to engage in cyberbullying.
  - Bypass Internet filter.
  - Use cell phones or other digital devices.
  - This raises liability concerns.

Who

- Known cyberbully.
- Cyberbullying-by-proxy—bully solicits involvement of other people who do not know the target.
- Anonymous.
- Impersonation for the purpose of getting someone else in trouble.
- Figuring out who
  - Generally, teens are not very good at hiding their identity.
  - Investigations to figure out who.
    - Other material posted.
    - Friendship links.
    - Interviews with less-involved students.
  - Law enforcement officials have greater ability to obtain identity information.

Relation to School Bullying

- Continuation of in-school bullying.
- Retaliation for in-school bullying.
- Victimization can lead to threats or distressing material.
- DO NOT immediately assume that the student posting the harmful online material is the originator of the problem.

- Look at 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 highly probable that this material is posted in retaliation for bullying or other emotional harm inflicted at school.

Social Status Issues

- Students most often involved in cyberbullying appear to be the “in-crowd” students.
  - “Wannabes” appear to be the most frequent targets.
  - These are students who are most actively interacting with each other online.
  - These are not the typical “bullies” as identified in the research literature.
- Losers and outcasts.
  - Appear to be less inclined to participate actively in the online social dynamics of the school community.
  - May be targets of indirect cyberbullying through denigration.
  - May be posting angry condemnations of the students and staff who denigrate them at school.
  - May form their own online troublesome groups or participate in unsafe or dangerous communities.

Boys or Girls

- Girls tend to be more actively involved in online communications, which is the venue for cyberbullying.
- Boys tend to be interested in gaming, violence against fictional characters.

Personal Relationships

- Harassment in the context of “flirting.”
- Relationship break-ups.
  - Sometimes, teens provide intimate images in the context of relationships and upon a break-up, this material could be disseminated.
- Online fights about relationships.

Hate or Bias

- Based on race, religion, obesity, or sexual orientation.
- Cyberbullying based on sexual orientation appears to be quite frequent.
  - Has been implicated/suggested in many of the cases that have resulted in suicide.

Roles

- Bullies.
  - “Put-downers” who harass and demean others they think are different or inferior.
  - “Get-backers” who have been bullied by others and are using the Internet to retaliate or vent their anger.
- Targets.
  - Students who are also being bullied at school.
  - Student who are bullying others at school.

- Harmful Bystanders.
- Helpful Bystanders.

Impact

- 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.

Cyberthreat Insight

- Unresolved conflict.
- Online gaming.
- Is it real?
- Leakage.
- Threat and suicide assessment.

Unresolved Conflict

- Students who are victimized at school—by students or teachers—who retaliate by expressing anger or threats online.
- And are then subjected to extreme punishment.
- This should be considered a school FAILURE!
- Student posting harmful material should be held appropriately accountable.
- But situation must be viewed in entire context and ALL participants must be held fully accountable.

Online Gaming

- Cyberthreats could be related to online role-playing gaming involvement.
  - Online role playing games frequently involve small groups of players developing plans for a violent attack within the simulated game.
  - Possibility this may be implicated in the recent phenomenon of groups of boys planning school violence.
  - Youth who are abused at school, "outcasts," or "at risk" in other ways who are also involved with online violent gaming.

Is it Real?

- Youth make threats all the time.
  - Their tone of voice, posture, overall interaction allow others to determine whether or not their expression is a “real threat.
- Just because material has been posted online does not make more of a threat.
- Online material that looks threatening could be:
  - A joke, parody, or game.
  - A rumor that got started and has grown and spread.
  - Material posted by a young person who is trying out a fictitious threatening online character.
  - The final salvos of a “flame war” that has gotten out of hand, but will unlikely result in any real violence.
  - Material posted by someone impersonating another someone else for the purpose of getting that person into trouble.
  - Distressing material posted by a depressed or angry young person that could foretell a violent or suicidal intention, but does not represent an imminent threat.
  - A legitimate imminent threat.
- Must respond in the most appropriate manner.
  - But continuous reassessment is necessary.
- Two messages to impart 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.
- Use “teachable moments,” such as news stories, to communicate this to students.

"Leakage"

- When a student intentionally or unintentionally reveals clues to feelings, thoughts, fantasies, attitudes, or intentions that may signal an impending violent act against self or others.
- Assume that an emotional distraught youth with Internet access will be posting material that provides insight into their mental state and the reasons for that mental state.

Threat and Suicide Assessment

- 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!

Targeting Staff

- Students posting harmful material targeting teachers or other staff.
- Could be a range of material:
  - Staff person is targeted because of some perceived status issue, such as sexual orientation or obesity.
  - Obnoxious attention-seeking student.

- "Youthful exuberance," a convenient target, and a lack of sensitivity to the harm caused.
- Legitimate objections to the actions or policies of the school or staff.
- Student legitimately feels that he or she has been bullied or mistreated by the teacher.
  - Must acknowledge that some school staff are bullying and denigrating students.

Legal Issues

- Search and seizure.
- Free speech.
- Liability.

Search and Seizure

- When can a school monitor and search student Internet use records and files?
  - No cases directly on point, but standards are generally well-accepted.
  - Users should have a limited expectation of privacy on the district's Internet system.
  - Routine maintenance and monitoring, (technical and by staff) may lead to discovery that a user has violated district policy or law.
  - An individual search will be conducted if there is reasonable suspicion that a user has violated district policy or the law.
- Schools should determine who has authority to authorize an individual search and record-keeping requirements.
- Clear notice to students that Internet use is monitored can enhance deterrence.
- What about cell phones or other personal digital devices—laptops, PDAs, digital cameras—used by students on campus?
  - Recent Federal case indicated review of cell phone records by school officials may violate state wire-tapping law.
  - Likely should be addressed by signed agreement or implied consent
    - If a student brings a personal digital device to school and it is used for instructional activities in class, the teacher has the right to review history of use.
    - If there is reasonable suspicion of misuse, school officials have right to review records.
    - Probable should have a retention and appeal process.

Free Speech

- When can a school respond to cyberbullying?
- *Tinker* Standard—school officials may intervene only when there is a substantial and material threat of disruption or interference with the rights of other students.
  - Has been applied to off-campus harmful online speech by students targeting staff and in most early cases, even with ugly speech, the court ruled against the district
  - Some legal commentators disagree and urge no right of school to intervene in cases of off-campus online speech.
  - But more recent cases have upheld school response indicating the school met the standard of material and substantial disruption.

- Personal opinion is that courts are going to be much more likely to support intervention if student is being harmed by the off-campus speech because there is clear research evidence of the harmful impact on students and potentially the school community (i.e. school shooters) when students are harmed by bullying.

- *Hazelwood* standard—school officials may impose educationally-based restrictions.
  - Applies to on-campus speech that occurs through a school-authorized forum, such as school newspaper.
  - Should apply to all speech disseminated through district Internet system, but might not if the district is allowing students to make use of the Internet in the manner of a public access system—"open use."
    - If *Hazelwood* does not apply, then *Tinker* would.
  - Applies to distance education programs and social networking tools used educationally.
- How can schools address free speech issues in cases of off-campus cyberbullying?
  - Document school nexus.
    - Relationship to in-school incidents.
    - Access to site while at school.
  - Document disruption, interference, or threat thereof.
- Three case studies.
  - Three students involved in a school altercation. One is African American. Principal thought situation addressed. Shortly thereafter, the two Caucasian students create a threatening racist profile on a social networking site, but no specific reference to the African American student. Other students at school link to the profile. African American student finds out, tells Black Student Union, and tells principal.
  - Female students at school create a "We Hate Ashley" profile that includes many significantly ugly comments about Ashley. Other students have linked to and are participating in comments posted to this site. Ashley's parents report site to school. Principal interviews Ashley. She appears emotionally stable and is doing fine in her class work.
  - Elementary school child is punched in stomach during recess, but does not report. Using his home computer, he posts a very nasty comment about the student who punched him, which also negatively implicates a teacher. At school, other students are nervous and discussing online posting.
  - Personal opinion is that a formal disciplinary response is justified in the first two cases based on threat of disruption. Threat is quite obvious in first case. The fact that Ashley currently appears to be emotionally stable presents uncertainty. But there have been several cases where the students targeted by cyberbullying physically attacked the bully at school—in one case resulting in murder. No formal disciplinary response is justified in third incident. But informal actions to remove harmful posting and resolve on-campus concerns are necessary.
- What about student use of cell phones on campus or use of personal digital devices in the classroom?
  - *Tinker* standard would most likely apply.

District Liability

- When must a school respond to cyberbullying or other concerns?

- District liability concerns are raised when cyberbullying or cyberthreats are occurring through district Internet system or via cell phone or other digital devices used on campus.
- Negligence cause of action.
  - Do schools have a duty to exercise precautions against student cyberbullying through district Internet system and through use of cell phones on campus?
  - Did the school fail to exercise a reasonable standard of care?
  - Was it foreseeable that students would use the district Internet system to cyberbully others?
  - Is there an actual injury?
- Statutory liability.
  - Federal and state civil rights statutes.
  - Has school effectively caused, encouraged, accepted, tolerated, or failed to correct a sexually or racially hostile environment of which it has actual or constructive notice?
  - "Constructive notice"—if upon reasonably diligent inquiry, school should have known of the discrimination.
- Personal opinion: what are "reasonable" steps?
  - Conduct a needs assessment to determine extent of problems related to misuse of the Internet, cell phones, and digital devices on campus.
  - Revise policies and Internet use management practices to address cyberbullying and cyberthreats.
  - Implement more effective practices to supervise and monitor student Internet use.
  - Educate students and teachers on the concerns of cyberbullying and cyberthreats.
  - Implement a cyberbullying and cyberthreat report, review, and intervention process.
  - Ongoing evaluation.

Comprehensive Approach

- Research-guided.
- Comprehensive planning.
- Needs assessment.
- Policy and practices review.
- Professional development.
- Parent outreach.
- Community outreach.
- Student education.
- Evaluation and assessment.

"Research-guided"

- Based on:
  - Best practices in bullying, violence, and suicide prevention programs.
  - Research insight into bullying.
  - Traditional threat assessment processes.

- Combined with:
  - Insight into online behavior of youth.
  - Legal analysis.
  - Comprehensive approach to manage Internet use in school and home.
- Not research-based.
  - If want to use Safe and Drug Free Schools funds will have to seek waiver of Principles of Effectiveness standard.
  - A continuous improvement approach.

Comprehensive Planning

- Safe schools committee.
  - Administrator.
  - Counselor/psychologist.
  - Technology director.
  - Librarian.
  - Community members – school security officer, parents, law enforcement, mental health organizations.
  - Students or separate student advisory committee.
- This approach will require a systemic change.
  - In most schools, technology services departments manage Internet use issues and have limited understanding of youth risk. Safe schools committees manage youth risk issues and have limited understanding of technology.
- District committee responsibilities.
  - Policies, overall district Internet use management, needs assessment, professional development, electronic communications to support school level personnel, online reporting system, evaluation, funding.
- School committees responsibilities.
  - Communication of policies to students, ensuring effective Internet use practices and monitoring, establishment of reporting and intervention process, professional development, student education, parent education, evaluation.

Needs Assessment

- May need to be done first, to convince people that there is a real problem.
- Conducting regular surveys can provide insight into the effectiveness of the program.
- Student survey.
  - On-campus or off-campus instances.
  - Relationship to on-campus actions.
  - Impacts.
  - Reporting concerns.
  - Attitudes, risk factors, and protective factors.
- Administrative survey.
  - Extent of perceived concerns.
  - Issues around current school policies.

- Internet use management issues.
- Reporting and response.

Policy and Practice Review

- Expand the bullying/threat report process to incorporate cyberbullying and cyberthreats.
  - Should be anonymous and/or confidential.
    - Concerns about online retaliation are very real.
  - Establish an online reporting form or email report.
  - Make sure students know to provide downloaded material and/or the URL where the harmful material has been found.
- Review policies and practices addressing cell phones and personal digital devices.
  - Any use on campus should be subject to disciplinary code.
    - Including anti-bullying/harassment and search and seizure.
  - Cell phone use in classroom generally not allowed.
  - But students will be using personal digital devices in classrooms for instructional activities.
- Review policies and practices addressing Internet use.
  - See more below.
- Establish cyberbully or cyberthreat situation review and intervention plan
  - See attached.
- Overall threat assessment process and suicide prevention planning should also address Internet communications.
  - If any suggestion of threat is reported or a student appears to be distressed, it is advisable to search online for additional material.

Professional Development

- "Triage" approach.
  - Key person in district/region/state needs high level of training.
  - Safe schools planning committee members and all "first responders" need insight into problem and ways to detect, review, and intervene, with back-up from key person.
  - All other staff need general awareness.

Parent Outreach

- Provide information on how to:
  - Prevent, detect and intervene if their child is victim.
  - Prevent their child from being cyberbully.
  - Possible consequences if child is a cyberbully.
  - Empower their child to be a responsible bystander.
- Provide information to parents through:
  - General information through newsletters.
  - Parent workshops.

- "Just-in-time" comprehensive resources in office and online because parents likely will not pay attention until they need the information.

Community Outreach

- Provide information and training to others:
  - Mental health and law enforcement professionals.
    - May be involved in responses to specific incidents.
  - Community and youth organizations.
    - Provide an additional avenue for communication to parents and students.
  - Media.

Student Education

- Prerequisite to addressing cyberbullying is effective social skills education.
- Students must understand Internet safety and responsible use issues and know how to prevent, detect, and respond to problems.
  - Cyberbullying prevention and responses.
  - Legal principles of online publishing.
  - Internet privacy and public disclosure concerns.
  - Reporting cyberthreats and not making cyberthreats.
  - Enhance inclination to be a helpful bystander.

Evaluation and Assessment

- Must be a continuous improvement approach.
  - Research insight on cyberbullying and other aspects of youth risk online emerging.
  - Technologies always changing.
  - Legal standards unclear.
  - Must respond now and not wait for a "research proven model."
  - But must constantly evaluate and modify the approach based on new insight and results of local efforts

Internet Use Management

- Concerns.
- Education purpose.
- Internet use policies.
- Internet use practices.
- Effective monitoring.

Concerns

- Significant concerns about the effective management of Internet use in schools.
- Current Internet use management.
  - Legalistic Internet use policy.
  - Filtering software.
  - Fear-based, simplistic education.

- Problems.
  - Policies are not generally read—or understood.
  - Filtering software can easily be bypassed. (Google: bypass, Internet, filter)
  - Younger students need better protection.
  - Teens must understand school rules and know how to prevent, detect, and respond to problems
- A more effective approach is grounded in a strategy to:
  - Prohibit or severely limit non-educational use of the Internet.
  - Protect elementary students.
  - Hold middle and high school students accountable through effective supervision and monitoring practices.

Education Purpose

- Internet use in schools should be for educational purposes only.
  - Classwork and independent research on subjects similar to what studied in school or resources in library.
    - This is necessary preparation for workplace. Internet use on the job should also be for work-related purposes only.
    - Increased professional and curriculum development is essential.
    - Restricting “Internet recess” will be difficult in some schools because “open use” is expected.

Internet Use Policies

- Tied to disciplinary code.
- Clearly communicated to staff and students.
- Foundation for student education.

Internet Use Practices

- Make sure Internet filter is not implemented in a manner that is discriminatory!
  - Many filters block access to high quality support sites for LGBTQ students.
- Provide access to previewed educational research resources sites.
- Allow access outside of educational sites for specific projects.
  - Extremely limited for elementary students.
  - Greater access at middle and high school level.
- Establish controlled communications environment.
- Specifically provide access to reviewed sites for sensitive health and well-being information.

Effective Monitoring

- Must shift from “blocking” approach to effective “monitoring.”
- Monitoring must be sufficient to detect most instances of misuse.
- Supervision of students by teachers is essential.

- Routine, variable checking of history file is one strategy.

- Technology-facilitated monitoring strongly advised.
  - Real time monitoring.
  - Intelligent content analysis.

Cyber-Savvy Schools

- The fact that concerning material is or can be preserved in electronic format, and the true author can generally be identified, provides significant advantages for cyber-savvy safe school personnel to more effectively discover and intervene in situations that are negatively impacting students.

State Planning to Address Youth Risk Online

- Recommendations:
  - Form state-level task force.
    - Department of Education, Safe Schools.
    - Department of Education, Educational Technology.
    - State Mental Health.
    - Attorney General's Office.
    - Education Leader's Associations.
  - Conduct needs assessment.
  - Revise state safe schools plan to address youth risk online.

Nancy E. Willard has degrees in special education and law. She taught "at risk" children, practiced computer law, and was an educational technology consultant before focusing her professional attention on issues of youth risk online and effective Internet use management in schools. Nancy frequently conducts workshops for educators. She is expanding her use of Internet technologies to deliver "virtual" presentations and classes. She is the author of two books: *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress* (Research Press) and *Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Use the Internet Safety and Responsibly* (Jossey-Bass).

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
© 2006 CRSIU
May be reproduced and distributed for non-profit purposes.