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
E-mail: nwillard@csriu.org

Keep in Mind

- If this were easy, we wouldn't be here!

Overview of Presentation

- Part I. Social Aspects
  - Cyberbullying and related concerns
  - Youth behavior online
- Part II. Comprehensive Approach to Address Concerns
- Part III (afternoon) How to Respond to Cyberbullying Without Getting Sued

Web 1.0 to Web 2.0

- Web 1.0 was largely one-directional
  - Web as information source
- Web 2.0
  - Participatory
    - All users can easily post information online and interact with others
  - Highly mobile
    - From desk-top to personal digital devices

Web 1.0 Internet Safety

- Fear-mongering
  - "One in 5 young people have been sexually solicited online"
- Simplistic rules
  - "Don't provide personal information online"
  - "Don't talk to online strangers"
  - "If something makes you uncomfortable, tell an adult"
- Overreliance on filtering
  - "Parental controls can protect your child online"

Web 2.0 Reality

- Fear is interfering with youth reporting of online concerns
  - Young people know adults fear the Internet
  - They are less likely to tell an adult when they are in trouble online, because they think the adult will overreact and restrict their access
- Tweens and teens must fully understand what the risks are and how to prevent and respond to risky situations online
- Filtering will not deter a determined teen or address communication concerns

Cyber-Safe Kids Cyber-Savvy Teens

- When children are younger, they need to use the Internet in safer places with simple guidelines
- As they grow, they need the knowledge, skills and values to independently make safe and responsible choices online
- Adults must remain engaged

Cyberbullying and Cyberthreats: What is it?

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
- Kids being mean to each other online

Different Forms

- Flaming
  - Online "fights" using electronic

messages with angry and vulgar language

- Harassment
  - Repeatedly sending offensive, rude, and insulting messages
- Denigration
  - Sending or posting cruel gossip or rumors about a person to damage his or her reputation or friendships
  - "Dissing" someone online
- 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
- 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
  - Use of technology, usually cell phone, to control a partner

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
  - Assume that an emotional distraught youth with Internet access will be posting material that provides insight into their mental state

Other Related Online Risks

Sexually Related Risks

- Sexual "hook-ups"
  - Teens using Internet to make connections for sexual activities
- 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
  - Self-cutting, anorexia, drug-use, suicide
  - Find acceptance from like-minded peers
  - Leads to contagion of unhealthy attitudes and behavior
- Recognize it is essential to create a safety plan for such teens and not simply cut off access

Dangerous Online Groups

- Angry teens becoming involved in hate groups or gangs with adult members and recruiters or forming their own troublesome youth groups
  - May be specifically recruited
  - Find acceptance from like-minded peers or adults
  - Leads to contagion of unhealthy attitudes and behavior

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 violent attacks at school

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
- Must learn to differentiate and protect
  - Personal contact information
  - Intimate material that could make them vulnerable
  - Reputation-damaging material

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 anxiety over acceptance and status
  - Addictive features of gaming environments
  - Lack of healthy peer connections
  - Likely new cause of school failure

Insight into Cyberbullying and Cyberthreat Behavior

How

- Any form of electronic communication
- Most frequently
  - Posted on social networking profile
  - Sent via social networking messaging, instant messaging, or text messaging
- Most sites and services have terms of use that prohibit posting harmful material and will remove harmful material or terminate use if a a complaint is filed

How Big a Problem

- Watch out for surveys
  - The degree of harm reported is related to how the questions are asked
    - And sometimes the motivations of the researchers
  - Surveys are not effectively distinguishing between minor and significant incidents
  - Surveys are not effectively defining harmful acts
- I-Safe (2004) (grades 4 - 8)
  - 42% have been bullied online
  - 35% have been threatened online
  - 21% have received mean or threatening e-mail or other messages
  - 58% someone said mean or hurtful things to them online
- Fight Crime: Invest in Kids (2006)
  - 30% of teens (12-17) and 17% of children (6-11) have had mean, threatening or embarrassing things said about them online
  - 10% of teens and 4% of the younger children were threatened online with physical harm
- Crimes Against Children Research Center (2006)
  - 9% of youth (10 and 17) reported they had been harassed online
    - But this figure excluded sexual harassment
- NSBA Creating and Connecting (2007)
  - 7% have experienced “self-defined” cyberbullying

Where

- Significant amount is occurring off-campus
  - More unsupervised time
  - But is negatively impacting student relationships on-campus
- Students are also using the district Internet system or personal cell phones to engage in cyberbullying
- Must focus on comprehensive prevention

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

- Teens are not very good at hiding 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
- In-school victimization can lead to online threats or distressing material

- DO NOT immediately assume that the student posting the harmful online material is the origin of the problem
  - Evaluate the substance of the communications
  - Look at the "social status" level of all of the participants
  - Determine the overall relationship issues

Address Underlying Conflict

- Students who are victimized at school ~ by students or teachers ~ are retaliating by expressing anger or threats online
  - Student who post harmful material should be held appropriately accountable
  - But situation must be viewed in entire context
  - ALL participants must be held fully accountable,
  - The underlying conflict must be addressed

Social Status Issues

- Appears to be closely linked to social status issues
  - Students who are active participants in the "social status drama" at school
    - Communicating with each other in online communities
    - "Queen Bees," "Kingpins," "Preps," "Wannabes"
- These are not the typical bullies as identified in the research literature
  - "School yard thugs"
- "Losers" and "outcasts"
  - Do not appear to be participating in the online social dynamics of these communities
  - May be targets of indirect cyberbullying
  - May be posting angry condemnations of the students and staff who denigrate them in some other location
  - 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
  - The venue for cyberbullying
- Boys tend to be interested in gaming
  - Violence against fictional characters
- Some surveys are showing greater involvement in cyberbullying by girls

Personal Relationships

- Sexual harassment in the context of "flirting"
- Relationship break-ups
- Online fights about relationships
- Use of telecommunications to control partners in unhealthy relationships
  - Especially cell phones

Hate or Bias

- Based on race, religion, obesity, or sexual orientation
  - Cyberbullying based on perception of sexual orientation appears to be quite frequent
    - Has been implicated/suggested in many of the cases that have resulted in suicide
  - Watch out for increase in "immigration status" cyberbullying

Helpful Bystanders

- Emerging research indicates that role of "friends" is critically important to emotional health of target and resolution of the problem
- Empowering bystanders will be a key prevention strategy
  - Powerfully influence social climate
  - Give the targets strength
  - Report serious concerns to adults

Impact

- The harm caused by cyberbullying may be greater than traditional bullying
  - Online communications can be vicious
  - There is no escape ~ victimization is ongoing, 24/7
  - Harmful material can be distributed worldwide and is often irretrievable
  - Cyberbullies can be anonymous, so the target may not know whom to trust
  - Cyberbullies can solicit the involvement of unknown "friends"

Reporting

- Young people are reluctant to tell adults
- They fear adults will

  - Not know what to do
  - Make matters worse
    - High potential for uncontrollable online retaliation
  - Restrict their online access
    - Akin to "excommunication"

Cyberthreats ~ 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 threatening material could be:
  - A joke, parody, or game
  - A rumor that has grown and spread
  - Fictitious threatening online character
  - The final salvos of a "flame war"
  - Someone impersonating another to get that person into trouble
  - Distressing material, but not an imminent threat
  - A legitimate imminent threat
- Must respond in an appropriate manner
  - But ongoing reassessment is necessary
- The manner in which you respond to a situation that was not a "real threat" will heavily influence the willingness of students to report suspected threats in the future
  - If it wasn't a real threat "back off"

Message 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

Targeting Staff

- Range of material
  - Staff person is targeted because of "status"
  - Obnoxious attention-seeking student
  - A convenient target and a lack of sensitivity
  - 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

Influences on Online Behavior

- Why do they do things that they would never do in the "real world?"
  - Brain development
  - Disinhibition
  - Exploration of identity
  - Emerging sexuality
  - Online social norms
  - Social influence used to manipulate
  - Spectrum of risk

Brain Development

- Didn't think
- In teens, the frontal cortex is restructuring
  - Frontal cortex supports rational, ethical decision-making
  - Learning to make good decisions requires paying attention to actions and consequences
  - Technologies interfere with the recognition of the consequences of actions

Disinhibition

- You Can't See Me ~ I Can't See You
- Perception of invisibility or creation of anonymity online …
  - Removes concerns of detection resulting in disapproval or punishment
- Lack of tangible feedback about the consequences of actions online …
  - Interferes with empathy and leads to the misperception that no harm has resulted

Exploration of Identity

- Who am I
- Teens are exploring who they are online
  - Number of links and amount of communication activity is new measure of social status and self-worth
  - High social anxiety can fuel addictive access and bad attention-getting choices
  - Public exploration of identity can lead to disclosure of highly intimate or reputation damaging material

Emerging Sexuality

- Am I hot?
- Teens are emerging sexually …
- They are exploring their sexuality and relationships through online communications
- What one teen considers "flirting" may be perceived as "sexual harassment" by the recipient

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"
- "If I can do it, it must be okay."
- "I have the free speech right to write or post anything I want, regardless of the harm it might cause to another"

Youth Risk Online

- Looking for Love
- Youth online risk must be viewed from perspective of adolescent risk
- Savvy ~ Naïve ~ Vulnerable ~ At Risk
- Savvy teens
  - Make good choices
  - Generally older
  - Applying "real world" values and common sense online
- Naïve teens
  - Make mistakes
  - Likely to be younger
  - Can become savvy with education and experience
- Vulnerable teens
  - Going through a period of "teen angst"
  - Higher risk online
- At risk teens
  - Face major ongoing challenges related to personal mental health and disruptions in relations with parents, school, and/or peers
  - Highest risk online
- The higher the degree of risk, the greater the probability the teens will be …
  - Searching for acceptance and attention from people online
  - More vulnerable to manipulation
  - Emotionally upset and thus less likely to make good choices
  - Less attentive to Internet safety messages
  - Less resilient in getting out of a difficult situation even if they want to
  - Less able or willing to rely on parents for assistance
  - Concerned about reporting an online dangerous situation to an adult because this could reveal evidence of their own unsafe or inappropriate choices
- Which means we must …
  - Educate adults who are likely in the best position to detect and respond to concerns involving higher risk youth
  - Develop effective teen "bystander strategies" to encourage competent teens to provide assistance to peers and report online concerns to adults

Legal Issues: In Brief

Boundaries of Schoolhouse Gate

- Authority
  - Legal right to impose formal discipline or restrictions
- Responsibility
  - Legal obligation to exercise reasonable precautions and to respond to reports of concerns

District Internet System

- School officials have the **authority** and **responsibility** to respond to any on-campus or off-campus harmful or inappropriate speech through the District Internet system
  - Have the ability to supervise and technically monitor

Personal Digital Devices

- School officials have the authority and responsibility to respond to any harmful speech that takes place while students are using personal digital devices on-campus
  - But ability to monitor and review is limited, so must depend on student report
  - And searching a student's cell phone or PDA without parent permission may violate state wiretapping laws

Off-Campus Speech

- School officials have the **authority** to respond to off-campus online speech that creates or threatens substantial disruption at school or interference with the rights of students to be secure or is a true threat
  - But not offensive speech and only rarely if speech targets staff

Off-Campus Speech

- School officials **may** have the **responsibility** to respond to off-campus online speech that has created a hostile environment at school for a protected class student, if they know of the concern
  - School officials definitely have a responsibility to respond if district Internet system was used or there are associated on-campus altercations

Parent Liability

- Parents can be held financially liable for the harm caused by their children
  - Parental liability statutes
  - Parental negligence
- Causes of action
  - Defamation
  - Invasion of privacy ~ disclosure of private face or false light
  - Intentional infliction of emotional distress

Criminal Violations

- Some cyberbullying meets the standards of criminal violations, including …
  - Threats
  - Coercion
  - Harassing telephone calls or text
  - Harassment or stalking
  - Hate or bias crimes
  - Child pornography
  - Sexual exploitation
  - Taking a photo of someone in a private place

Comprehensive Approach

- Not scientifically-based research
  - Insufficient research into concern
  - Technologies keep changing
- Based on Olweus Bullying Prevention
  - Modified to address technical and legal challenges
  - Likely will always be a “moving target”
- Requires a continuous improvement approach
- SDFSCA Requirements
  - “A local educational agency may apply to the State for a waiver of the requirement of (Principles of Effectiveness) to allow innovative activities or programs that demonstrate substantial likelihood of success” [Section 4115 (c)
  - Comprehensive approach incorporates elements necessary to achieve waiver

Comprehensive Planning

- Administrators
- Counselors/Psychologists
- Educational Technology
  - Technology Services
  - Educational Technology Staff/Librarians
- School Resource Officers
- Community Mental Health
- A merger of safe schools and educational technology is essential
  - Technology services departments manage Internet use technical issues
    - Generally do not fully understand youth risk
  - Educational technology staff/librarians teach Internet use issues
    - May not fully understand youth risk
  - Safe schools committees address youth risk
    - Generally do not fully understand technologies or what students are doing online
- District committee responsibilities
  - Policies
  - Overall district Internet use management
  - Needs assessment
  - Professional development
  - Online reporting system
  - Evaluation
  - Funding
  - Support for school level committees and personnel

- School committees responsibilities
  - Communication of policies to students
  - Ensuring effective Internet use practices and monitoring
  - Establishment of school-based 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
  - But anticipate cyberbullying reports to go up due to increased reporting

Policy and Practice Review

- Expand the bullying/threat report process to incorporate cyberbullying and cyberthreats
- Establish cyberbully or cyberthreat situation review and intervention plan
- Revise threat assessment process and suicide prevention planning to address Internet communications.
- Internet use
  - Students can easily bypass the filter to get to sites to engage in cyberbullying
    - Search: "bypass Internet filter"
  - Overreliance on filtering has resulted in
    - Too much Internet "recess"
    - Insufficient supervision and technical monitoring
  - Significant concerns with 1:1 laptops
    - Especially if school computers go home
- Internet use
  - Restrict use of District Internet to educational activities
    - Class work, extra credit projects, approved independent studies or activities
    - Provide professional development and technology resources
  - Ensure effective supervision
  - Increase use of technical monitoring
  - Closely evaluate and rethink 1:1 laptops
- Personal digital devices
  - Students are being cyberbullied, but will not report because using cell phone at school is a violation of school policy
  - It is probably a violation of state wiretapping law to review the electronic records on a cell phone or PDA without adult consent
  - Prepare for the fact that students will have PDAs with full computing and Internet access capabilities that they will want to use in the classroom for note taking and research

Cyberbullying Policy

- Bullying or harassment that takes place on or immediately adjacent to school grounds, at any school-sponsored activity, on school-provided transportation or at any official school bus stop, through the use of the district Internet system while on or off-campus, through the use of a personal digital device on campus, or off-campus activities that cause or threaten to cause a substantial disruption at school.
- "Substantial disruption" means:
  - Significant interference with instructional activities, school activities, or school operations
  - An environment for any student that is abusive, intimidating, threatening, or hostile and impairs that student's ability to participate in educational programs or school activities
  - Physical or verbal violent altercations between students

Professional Development

- "Triage" approach
  - Key district individuals
    - Require high level of understanding
    - Social, technical, legal
    - Serve as resource to other district personnel
  - Safe school and ed technology staff
    - Require good level of understanding
  - All others
    - Awareness

Parent Outreach

- Provide information on how to
  - Prevent, detect and intervene if their

child is target
  - Prevent their child from being cyberbully
    - Possible consequences if child is a cyberbully
  - Empower their child to be a responsible bystander
    - The parents most likely to pay attention likely have savvy children who can be effective bystanders
- Provide information to parents through
  - General information through newsletters
  - Parent workshops
  - "Just-in-time" comprehensive resources in office and online

Community Outreach

- Provide information and training to others
  - Mental health and law enforcement professionals
    - May be involved in specific incidents
  - Community and youth organizations
    - Additional vehicle to educate parents and students
  - Media
    - General community awareness

Student Education

- Effective social skills education foundation
- Cyberbullying prevention and responses
  - Target
  - Bully
  - Bystanders

Targets

- Prevention
- Do not post material that can be used against you
- Communicate respectfully to others
- Participate in online communities that have good values
- Address any bullying problems at school

Targets

- If Cyberbullied
- Never retaliate!
- Save the harmful material
- Self-help steps
  - Calmly tell the cyberbully to stop
  - Ignore or block the communications
  - File a complaint with the website

Targets

- Ask for help if these steps do not work or cyberbullying is significant
- Other response options
  - Send online material to parent of the cyberbully with a demand that it stop
  - Work with your school
  - Contact an attorney or the police

Bullies

- Prevention
- Emphasize importance of treating others kindly online
- Parents can be held financially liable for harm caused by their child

Bystanders

- Encourage students
  - Promote respectful communications
  - Assist others if they are being cyberbullied
  - Tell a trusted adult

Evaluation and Assessment

- A continuous improvement approach
- Ongoing assessment and evaluation
- Must constantly evaluate and modify the approach based on new insight and results of local efforts

Review and Action Options

- Situation Review
- Imminent Threat
- Evidence Gathering
- Violence or Suicide Assessment
- Cyberbully Assessment
- School Response Options
- Other Response Options

Situation Review

- Review team members could include an administrator, counselor/psychologist, technology coordinator, librarian, school resource officer, and community mental health resource
  - However, for most incidents, this entire team will likely not be needed

Imminent Threat

- Contact law enforcement and initiate a protective response
  - But continue with the following evidence gathering steps

  - Watch out for all of the possible alternatives

Evidence Gathering

- Preserve all evidence
- Determine the identity of cyberbully(ies)
- Search for additional harmful material
  - Conduct analysis of all involved students through District Internet system.

Violence - Suicide

- Does evidence gathered raise concerns that student(s) may pose a risk of harm to others or self
- Recognize that the threat of violence or suicide may come from student(s) who posted the material or from student(s) who were victimized

Cyberbully Assessment

- Determine whether the school can respond with formal discipline
- Get to a “root cause” understanding of the relationships and issues between the participants

School Response Options

- Formal discipline
- Informal resolution with parents.
- It is still essential to…
  - Ensure removal of materials
  - Prevent continuation or retaliation by the student or online “buddies”
  - Address the support needs of the target

Other Response Options

- Response option for students, parents, or staff, with or without formal discipline, include …
  - Calmly and strongly tell the cyberbully to stop
  - Ignore the cyberbully
  - File a complaint with the web site, Internet service provider or cell phone company.
  - Have the parents of the target contact the cyberbully’s parents or contact an attorney
  - Contact the police

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