Cyberbullying and Cyberthreats

Nancy Willard

Monday August 15th
2:00 PM – 3:15 PM
Washington 4

Cyberbullying and Cyberthreats

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

Part I. Overview of Cyberbullying and Cyberthreats

- Cyberbullying is disseminating harmful or cruel speech or engaging in other forms of social cruelty using the Internet or other information communication technologies
- Cyberthreats are either direct threats or material that raises concerns a young person may engage in an act of violence against others or self disseminated using the Internet or other information communication technologies

Types of cyberbullying activities

- Flaming
  - Sending angry, rude, vulgar messages
- Harassment
  - Repeatedly sending offensive messages
- Cyberstalking
  - Repeatedly sending threats of harm or highly intimidating messages
- Denigration (put-downs)
  - Posting untrue or cruel statements
- Impersonation
  - Pretending to be someone else to make that person look bad or place in danger
- Outing and Trickery
  - Posting material that contains sensitive, private information about another person or forwarding private messages
  - Engage in tricks to solicit embarrassing information that is then made public
- Exclusion
  - Intentionally excluding a person from online group

What and where

- Types of speech
  - Text, photos, drawings, videos, and audio
- Manner of dissemination
  - All forms of web publishing and electronic communication
  - Personal and third party web sites – sites to post material, generally more static
  - Blogs (weblogs) – interactive personal diaries
  - Email – asynchronous communication sent to individual(s) or a discussion list
  - Discussion groups – asynchronous group communications around a topic, students establish discuss groups that are school-related
  - Chat – synchronous group communication, with ability to have private chats
  - Instant messaging (IM) – synchronous private communication
  - Text/digital image messaging – messages or images sent via cell-phones
- Social networking communities, which combine many of the above features, are all the rage with teens
  - Look at http://www.myspace.com, http://www.bolt.com, http://studentcenter.org

Important insights about online environments

- Web site or provider Terms of Use generally prohibit harmful speech
  - But if not reported, can't be enforced
- Many sites have age limits older than 13
  - But youth know they can easily lie
- Filtering software is not effective in controlling cyberbullying and leads to false security

Conditions that appear to precipitate cyberbullying

- Face-to-face bullying
  - Continuation of or retaliation for ...
- Relationship issues
  - Failed relationships

  - Relationship-based fights
- Entertainment value
- Others?

Related youth high risk online behavior

- Key point: Teens who do not have strong "real world" connections appear to be the ones most attracted to these risky behaviors
- Disclosure of highly sensitive personal information, images, and perspectives
  - Limited understanding of public, permanent, transferable nature of disclosures or the risks
- Risky sexual behavior
- Suicide and self-harm "encouragement" communities
- Hate group recruitment and "gang" formation
- Violent gaming, sexual or biased-base victims

Part II. I Can't See You, You Can't See Me

- How does use of information and communication technologies impact behavior?

External forces that promote responsible behavior

- As young people are growing, three key external forces promote responsible behavior
  - Empathic recognition
  - Social disapproval
  - Negative consequences imposed by authority
- Eventually (hopefully), young people develop internalized control grounded in personal values
- Young people are using the Internet before full development of internalized control

Rationalizations

- Rationalizations are arguments people use to justify behavior that is not in accord with personal moral values or social expectations
- Common rationalizations
  - "I won't get caught"
  - "I didn't really hurt anyone"
  - "Everyone does it"
  - "He started it"
  - "She deserves it"
  - "He told me to"

Impact of information and communication technologies

- No tangible feedback
  - Reduces impact of empathy and recognition of harm – "I didn't really hurt anyone"
- Perception of invisibility
  - Reduces threat of negative consequence or social disapproval – "If I can't get caught, it's OK."
- Social norms support harmful online speech
  - "On the Internet, I have a free speech right to say whatever I want, without regard for the possible harm to others"
- Multiple online identities and personalities
  - "It wasn't really me, it was my persona"
- Simulation, role-playing, game playing environment
  - "Life on the screen is all just a game"
- Change in power balance
  - Less powerful person feels more comfortable in challenging more powerful person

Part III. Bullying and Threat Behavior

- Significant need for more data and analysis

Definition of bullying

- Face-to-face
  - Behavior intended to harm or disturb
  - Occurs repeatedly over time
  - Imbalance of power
- Cyberbullying
  - Same intent to harm and repeated nature
  - Online communications can change power balance providing greater opportunity for victim to retaliate
  - Must distinguish between "put down" and "get back" material

Bullying actions

- Face-to-face
  - Physical
  - Direct verbal
  - Indirect relationship aggression
- Cyberbullying
  - No physical form
  - Direct verbal includes flaming, harassment, cyberstalking
  - Indirect includes denigration, outing, trickery, impersonation, exclusion

Bully and victim profiles

- Face-to-face
  - Bullies
    - Alpha-wolf (social climber)
    - Aggressive bully
  - Victims

  - Passive victims
  - Provocative victims
  - Victim/bully
- Cyberbullying
  - Appears to be a lot of social climbing cyberbullying
  - Victims are retaliating online

Girls and boys

- Face-to-face
  - Frequently sated: "Boys bully more than girls"
  - But probably failure to recognize socially harmful acts of girls as bullying
- Cyberbullying
  - No physical bullying
  - Girls are involved more in online communication (boys play games)
  - Reportedly, more girls are cyberbullying

Bullying and sexual harassment

- Face-to-face
  - Sexual harassment sometimes included in definition of bullying, sometimes not
- Cyberbullying
  - Appears to be a significant amount of sexual-related harassment
  - Gender orientation harassment
  - Failed relationships, online or offline
  - Relationship-based arguments

Bullying motivated by hate and bias

- Face-to-face
  - Bullying can be based on race or religion bias
- Cyberbullying
  - Online hate group recruitment
  - Disaffected youth are attracted
  - Youth are forming their own hate-based online social communities
  - Online games reinforce bias-based hate

Bystanders

- Face-to-face
  - Bystanders reinforce bullies and maintain social norms
  - Emerging focus in bullying prevention is empowering bystanders to disapprove, intervene, and/or report
- Cyberbullying
  - No responsible adults are present in the online environments
  - Empowering online bystanders to disapprove, assist, and/or report will be essential!

Family dynamics

- Face-to-face
  - Parents of bullies demonstrate lack of involvement, no limit setting and model aggressive problem-solving
- Cyberbullying
  - Frequent Internet use survey finding: Parents are not involved in their children's online activities
  - Promotion of filtering software to "protect kids" has lead to false security and lack of involvement

Media influences

- Face-to-face
  - Media glorifies bullying and violence
- Cyberbullying
  - Some web sites encourage outrageous content or conduct because it draws traffic
  - Teens can be star of their own "reality TV" show
  - Game violence becomes personal violence, or all online violence is just a game

Incident rates

- Face-to-face
  - Depends on how the questions are asked and how the data is gathered
- Cyberbullying
  - A few brief surveys all ask the questions in different ways and report different results
  - 2004 US study reported 42% of youth in grades 4 – 8 said that had been bullied, 57% said someone had said something mean, 35% said they had been threatened
  - By all indications, a growing problem

Impact on victims

- Face-to-face
  - Victims and bullies suffer poor psychological and social adjustment
  - Can lead to suicide, self-harm, and violence
- Cyberbullying
  - Probably more emotionally damaging
  - Occurs 24/7, with wide, rapid distribution of material that can be impossible to remove
  - Bullies can be anonymous and solicit help from unknown buddies
  - Social norm against reporting to adults
- Are emerging reports of suicide and school violence related to cyberbullying
- Important: If you are working with a teen who is seriously depressed, demonstrating suicidal intentions, suicide attempt, etc. it is critically important to find out what is happening to that child online!

Cyberthreats

- Face-to-face
  - Youth make threats all of the time
  - Tone of voice, posture, overall interaction allow others to determine whether or not expression is a "real threat"
- Cyberthreats
  - Threat communicated online could be real or NOT
  - Just because it is written and communicated electronically, does not make it "more real"
- Be careful, online material could be
  - Good-natured fun, joke, parody
  - Nuisance activity
  - An online game or role-playing
  - Impersonation to get someone in trouble
  - Last chapter in an escalating fight
  - Hormonal outburst that came and went
  - Cry for help, intense anger
  - Imminent threat of violence to self or others
  - Other?

"Leakage"

- "Leakage" occurs when a student intentionally or unintentionally reveals clues to feelings, thoughts, fantasies, attitudes, or intentions that may signal an impending violent act. (FBI)
- One of the most important clues that may precede a violent act

- Cyberthreats
  - Technology facilitates open disclosure
  - Assume that emotional distraught youth with Internet access will be posting material that provides significant insight into their mental state
  - We must learn how to find, analyze, and effectively respond to online "leakage"
  - We must specifically encourage youth to identify and report online "leakage"

Part IV. Legal Issues

Search and seizure

- When can a school monitor and search student Internet use records and files?
- The "locker standard" applied to Internet use
  - Users 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 individual search and record-keeping
- Clear notice can enhance deterrence

Free speech issues

- When can a school respond to cyberbullying?
- The First Amendment places restrictions on public officials when intervening in situations involving expression of speech by students
- *Tinker* standard
  - Standard: School officials may intervene only when there is a substantial and material threat of disruption
  - Has recently been applied to off-campus online speech by students that relates to the school
  - But some legal commentators disagree
- *Hazelwood* standard
  - 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 speech disseminated through district Internet system and campus use of cell phones
- Off-campus online harmful speech cases
  - All but one case—speech directed at staff
  - All cases—decided based on *Tinker* standard
  - All but one case—the district settled or lost
  - In one case — the district won because the student had accessed the site from school and the teacher was very emotionally upset
  - No cases—addressing really serious student-to-student harmful online speech
- If off-campus online speech of a student has caused a material and substantial disruption in the life of another student, can the school respond? Unknown
- Will *Tinker* will continue to apply? Unknown
- How can schools handle the unknowns? Search diligently for, and document, school "nexus" to bring case under *Hazelwood* standard
  - Material posted or sent through district Internet system
  - Material displayed to other students through district Internet system
  - Material originated on-campus
  - Relationship with on-campus bullying
- If school "nexus" can't be found, support victim, contact parents to seek informal resolution, recommend civil litigation, or contact police

District liability

- When must a school respond to cyberbullying?

- District liability concerns are raised when cyberbullying or cyberthreats are occurring through district Internet system or via cell phone on campus

- Negligence claim
  - Duty to protect
  - General: Duty to anticipate foreseeable dangers and take necessary precautions
  - Specific: Children's Internet Protection Act requires policy that addresses safety of students using electronic communication
  - MPO (my professional opinion) Schools have a duty to exercise precautions against student cyberbullying through district Internet system and through use of cell phones on campus
  - Failure to exercise a reasonable standard of care
  - How would a "reasonable" educator in a similar situation have acted?
  - Has the district established a reasonable level of supervision/monitoring of student use of the Internet and provided a vehicle to report and respond to cyberbullying activity?
  - MPO Most districts have not established a reasonable level of monitoring and do not have effective reporting/response
  - Proximate cause
  - Was the student's injury foreseeable? Was there as a connection between breach of duty and injury?
  - Was it foreseeable that students could be using the district's Internet system to post to send harmful material to other students and did the lack of supervision/monitoring allow such an injury to occur?
  - MPO It is entirely foreseeable that students are using the district Internet system to cyberbully others, whether there is a connection will depend on facts
  - Actual injury
  - Was there a physical/emotional injury?
  - MPO Will depend on the facts
- Statutory liability
  - Civil rights statutes
  - Title IX of the Education Amendments of 1972
  - Title VI of the Civil Rights Act of 1964
  - State civil rights statutes
  - A violation of Title IX and VI may be found if a school has effectively caused, encouraged, accepted, tolerated, or failed to correct a sexually or racially hostile environment of which it has actual or constructive notice
  - A school is charged with constructive notice of a hostile environment if, upon reasonably diligent inquiry in the exercise of reasonable care, it should have known of the discrimination
  - Is the district being reasonably diligent in ensuring that students are not using the district Internet system in a harmful manner?

Civil litigation by victim

- When should parents pursue civil litigation against the bully and parents of the bully?
- Civil laws provide the ability for victims to sue perpetrator or perpetrator's parents to recover damages for injuries or require actions, such as removal of material and discontinuation of actions
- Cyberbullying could meet the standards for "intentional tort"
- Civil law theory 1: Defamation
  - Intentional publication
  - Of a false statement
  - That damages the victim's reputation in the community
  - A public official, such as a principal, must prove malice (person knew statement was false or was reckless in verifying truth)
  - Defense — published statement is true
  - A child's reputation is worthy of protection
- Civil law theory 2: Public disclosure of private fact
  - Public disclosure of a private fact that would be highly offensive to a reasonable person
  - Defenses — information is newsworthy or the victim gave consent
  - Activities of minors are generally not newsworthy and minors can't give legal consent
- Civil law theory 3: False light in the public eye
  - Person is placed before the public in a false light that would be highly offensive to a reasonable person
  - Defenses — information is newsworthy or the victim gave consent
  - Activities of minors are generally not newsworthy and minors can't give legal consent
- Civil law theory 4: Intentional infliction of emotional distress
  - A person's intentional or reckless actions are outrageous and intolerable and have caused extreme distress
- Civil law remedy 5: State laws may provide private right of action if a criminal act has been committed
  - For example, state hate crimes laws may provide right of private action
- Holding parents liable
  - Negligent supervision
  - A civil law cause of action
  - Parents have a duty to use reasonable care to supervise their children when they know, or

should know, of the necessity to exercise control and if they have the ability/opportunity to exercise such control
  - May require notice of prior inappropriate online actions and subsequent failure to supervise or intervene
  - Parental liability for intentional acts of minors
  - A state statute in almost all states
  - If child commits intentional tort, parents can be held liable regardless of parental action or inaction
  - Financial limits on amount recovered
- Filing civil action in small claims court
  - Financial limitation on damages, varies by state
  - Injunctive relief is possible, such as requiring an action or ceasing an action
  - No need for an attorney
  - But parents/victim will need some level of sophistication to prepare and present a case
  - Courts will not be familiar with use of small claims procedure for this activity

Criminal laws

- When should a school contact, or assist a parent in contacting, law enforcement officials?
- Federal criminal laws
  - 18 USC § 875. Extortion and threats sent through interstate communications
  - 18 U.S.C. 2425. Use of interstate communications to transmit information about a minor (for sexual purposes)
  - 47 USC § 223. Obscene or harassing telephone calls in interstate communications
- Will generally involve federal laws only if a really serious event
- State criminal laws — will vary by state
- Look for state criminal laws involving
  - Threats of violence
  - Harassment or stalking
  - Hate or bias crimes
  - Material harmful to minors, child pornography, or sexual exploitation
  - Taking photo in private place

Part V. Cyberbully or Cyberthreat Situation Review

- Not all cyberbullying will reach the level of cyberthreat, but some could
  - The threat could come from creator(s) or victim(s)
  - Threat could be to others or to self
- If material possibly presents a threat or "looks really bad"
  - Conduct a threat assessment
  - Call legal authorities, at any stage of the review process, if there is a possibility of a legitimate threat of violence to others

Review team

- Members
  - Administrator
  - School counselor or psychologist
  - Technology coordinator
  - Librarian
  - School resource officer
- Entire team may not be needed in all cases
- Helpful if the district has a key, knowledgeable person to assist with such cases

Step 1. Preserve the evidence

- Preserve initial evidence on district Internet system
- Instruct parents/student/staff how to preserve evidence on home computer/device and importance of doing so
- Offer technical assistance, if necessary

Step 2. Seek to identify creator(s)

- Obtain assistance of district technical services personnel
- Offer technical assistance to parents to identify unknown creator(s), if communication is coming to home computer/device
- Remember the possibility of impersonation
- Identification may not be immediately possible

Step 3. Search for Additional Material

- Search should include all participants
- Conduct search of files and Internet use records through district Internet system even if it appears to be off-campus activity, might find school "nexus"
- Conduct an additional search on the Internet including (librarian)
  - Online environment where initial material appeared
  - Search engine search for name and persona of student, friends, enemies, school name
  - Online communities used by students in your school

Step 4. Determine whether the school can respond directly

- Is there a school "nexus?"
- Is there a material and substantial threat of disruption?

- But even if a direct, disciplinary response is not justified, there are things a school can do

Step 5a. Evaluating speech directed at staff or school

- What is the nature of the material?
  - Nuisance activity
  - Legitimate protest speech
  - Fully protected speech, learn from it
  - "Put down" material, targeting teacher for perceived "negative" feature
  - Support teacher in responding
  - "Get back at" material, angry retaliation against teacher
  - Must ask why student is retaliating

Step 5b. Evaluating material directed at student(s)

- Is it "put down" material?
  - Possible continuation of face-to-face bullying
- Is it "get back at" material?
  - Possible retaliation for face-to-face or cyberbullying
- Need to get to "root cause" understanding of relationship

Threat assessment process

- FBI guidance: All threats are NOT created equal. However, all threats should be assessed in a timely manner and decisions regarding how they are handled must be done quickly.
- Follow Steps 1 - 3 discussed above
- Recommend Step 3 for all threats

Threat assessment questions

- If a threat is conveyed electronically, there is a tendency to think it is more legitimate than it really is, so these questions are really important in sorting out the situation
- FBI imminent threat questions:
  - Does the threat contain specific, plausible details that indicate that substantial thought, planning, and preparatory steps have already been taken?
  - If violence is threatened against others is the identity of the victim(s) and the reason for making the threat revealed?
  - Does the threat include specific information about the means or method of accomplishing the violent act and the time, place where the threatened act will occur?
  - Are there concrete indicators that planning and preparation has occurred?
  - Are the details logical and plausible?
  - Is there a realistic chance of carrying such a threat out to conclusion?

Emotional stability of participants

- Assess the emotional stability of the creator(s) and the victims(s)
  - If the material is "put down" material, the victim(s) may present risk or be at risk of committing violence to others or self
  - If the material is "get back at" material, the creator(s) likely present greatest risk and are at greatest risk
  - But there is a significant likelihood that "get back at" creator(s) have been victimized by the targets of the threatening material

Part VI. Cyberbully Intervention Strategies

- Schools must respond appropriately to on-campus cyberbullying
- There are ways that schools can respond to totally off-campus cyberbullying that is emotionally damaging a student

Intervention options

- For speech with school "nexus," use disciplinary process
  - Consequences should include ongoing specific monitoring of Internet activities
  - May also need to assist with other intervention actions to remove material or remedy harm
- For purely off-campus speech
  - Offer counseling support for victim, addressing emotional harm and empowerment
  - Seek informal resolution with parents of bully
  - Provide assistance to victim and parents in pursuing other actions

Informal resolution strategies for off-campus

- Contact parents of creator(s) and request their assistance in investigating and addressing their harm their child has been causing online
- Assume parents are unaware, will be disturbed, and will work with you
- Inform parents about potential legal consequences
- Provide parents with assistance in gaining supervisory control over child's Internet use
  - Including technical assistance in installing and using monitoring software, if appropriate
- Watch out — contact with parents could trigger retaliation against victim

Remove or stop speech

- If speech through district network or speech directed at staff, take actions to remove/stop
- Advise students/parents/staff how to remove/ stop speech and offer assistance, if necessary
- Techniques to remove or stop speech
  - Offensive speech is probably a violation of Terms of Use of site or provider
  - Find site or provider
  - Find Terms of Use and complaint procedures
  - Provide documentation of harmful speech
  - Request removal of material and termination of account
  - Recognize this may not totally solve problem, because creator can set up another account
- Other techniques
  - Use block function of communication tool
  - Change email address, screen name, email provider, phone number
- Students may resist removing themselves from the environments where they are being abused

Inform about civil legal action

- Provide information to parents/staff about possible civil legal action
  - A cease and desist letter from an attorney may be enough to stop the actions

Contact police

- Contact police or advise parents to contact police if speech involves
  - Death threats or threats of violence
  - Excessive intimidation or extortion
  - Hate crime
  - Sexual exploitation
  - Inappropriate images

Part VII. Comprehensive School and Community-based Approach to Address Cyberbullying and Cyberthreats

- Research-guided approach, 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 yet research-based
  - If using federal safe schools funds, must request waiver of Principles of Effectiveness

Comprehensive planning through safe schools committee

- School leaders
  - Administrator, counselor/psychologist
- Technology director
  - Safe schools committee should have responsibilities for student Internet use
- Librarian
- Community members
  - School security officer, parents, law enforcement, mental health organizations
- Students
  - Probably important, but potentially problematical because students could be viewed as traitors

Needs assessment—bringing "sunlight" to the problem

- Student survey to address
  - On-campus or off-campus instances
  - Relationship to on-campus actions
  - Impacts
  - Reporting concerns
  - Attitudes, risk factors, and protective factors
- May need to be done first, to convince people that there is a real concern
- Needs assessment survey is available from CSRIU

Policy and practice review

- Establish/expand bullying/threat report process
  - Anonymous and/or confidential because concerns about online retaliation are very real
  - Establish an online reporting form or email report
- Review cell phone/PDA policies and practices
  - Misuse should lead to discipline for bullying and ban on device at school.
- Review Internet policies and practices (see below)
- Establish cyberbully or cyberthreat situation review and threat assessment process
  - Overall threat assessment process must also address Internet communications – if any threat is made, search for additional material online
- Establish cyberbullying intervention process

Professional development

- "Triage" approach
  - Key person in district/region/state needs high level of training

- Safe schools planning committee and all "first responders" need insight into problem and ways to detect, review, and intervene, with back-up from key person
- Electronic communication within state
- All other staff need general awareness

Parent and community outreach

- Provide information on how to:
  - Prevent, detect and intervene if child is victim
  - Prevent child from being cyberbully
  - Possible consequences if child is a cyberbully
  - Strategies to empower and activate bystanders
- 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
- Provide information and training to others
  - Mental health professionals
  - Faith-based organizations
  - Youth organizations
  - Public library and community technology centers
  - Media

Student education

- Prerequisite to addressing cyberbullying is effective social skills education
- Educational approach should foster internalized values and character and empowerment of victims and bystanders
  - While it is necessary to improve monitoring and apply consequences, a behavior-management approach to education will not work because cyberbullying is occurring in online environments where there are no responsible adults
  - Enhance predictive empathy skills
  - Teach ethical decision-making skills
  - Teach conflict resolution and peer mediation
- Enhance understanding of legal principles for online publishing
- Address Internet privacy, public disclosure, and safety concerns
- Provide encouragement for reporting cyberthreats

Evaluation and assessment

- Ongoing evaluation is critically important
  - Cyberbullying is an emerging concern in a new environment that is not fully understood
  - Evaluation should inform implementation
- Performance measures approach
  - Performance objectives – tie to needs assessment findings
  - Inputs — resources allocated to the activities
  - Activities — specific program activities or tasks
  - Outputs — direct products of the program activities
  - Outcomes — consequences of the program on the intended recipients

Part VIII. Comprehensive Internet Use Management

- Needs assessment survey will reveal if there is a problem with student use of the Internet
- Misplaced reliance on filtering technology
  - Blocking does not totally prevent access to pornography and other bad stuff
  - Will not work to prevent cyberbullying
  - Has led to false security and failure to pay attention to what students are doing online
- A more comprehensive approach is essential
- Districts with laptop programs are especially at risk due to unsupervised home use of Internet

Basic approach

- Protection for younger students shifting to accountability reinforced by monitoring for older students
- Keep elementary students in safe places
  - Pre-reviewed sites
  - Open and transparent communications
  - Address Internet safety and responsibilities
- Shift at middle school to an accountability reinforced by monitoring approach
  - More intensive education about Internet safety and responsibilities
  - Strong focus on accountable actions in accord with district Internet policy
  - Effective technical monitoring

Focus on the educational purpose and use

- Increase use for high quality educational activities
- Decrease "Internet recess"
  - We all know what happens during recess
- Requires professional and curriculum development
- Educational technology-based instruction should be coordinated by curriculum and instruction department, not the technical services department

Clear, well-communicated policy

- Addressing
  - 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
- Internet use policy should be in line with all other disciplinary policies
- Under direction of safe school committee

Supervision and monitoring

- Important for deterrence, detection, investigation, and response
- Monitoring should be sufficient to establish the expectation that there is a high probability that instances of misuse will be detected and result in disciplinary action
- Intelligent content analysis technical monitoring is the best approach
  - Technology monitors all traffic and report on traffic that has elements that raise a "reasonable suspicion," allowing administrator to review reports.
  - Works in accord with "search and seizure" standards
  - Notice of monitoring will help to deter inappropriate activity
  - But no technology is perfect and students should be told not to rely on monitoring and to report any concerns

Appropriate discipline

- Fully integrated into school disciplinary response process

Conclusion: Essential question

- How can we raise kids to make the "right choices" when using information and communication technologies, choices based on internalized values grounded in respect for self, others, and the common good?

About the Presenter

Nancy Willard has degrees in special education and law. She taught "at risk" children, practiced computer law and was an educational technology consultant before focusing her professional attention on issues of youth behavior when using information communication technologies. Willard frequently lectures and conducts workshops for educators on policies and practices to help young people engage in safe and responsible use of the Internet and has written numerous articles on this subject. She is currently developing a research-guided strategy for schools, working in partnership with parents and community, to address concerns of cyberbullying and cyberthreats.

Willard is becoming affiliated with the Educational Development Center in Newton Massachusetts, to further her work in addressing cyberbullying, cyberthreats, and related Internet use concerns. EDC's vast background in the development and implementation of research-based violence prevention, anti-bullying, and suicide prevention programs will provide an important foundation for this work.

Center for Safe and Responsible Internet Use

The Center conducts research and provides resources and professional development to school districts to address issues related to the safe and responsible use of the Internet by students. The primary focus of the Center is on addressing concerns of cyberbullying and cyberthreats.

The following resources are available on the Center's Cyberbullying web site at http://cyberbully.org

- Parent's Guide to Cyberbullying and Cyberthreats
- Educator's Guide to Cyberbullying and Cyberthreats
- Cyberbully NOT student curriculum materials
- Cyberbullying and Cyberthreats Needs Assessment Survey

The following professional development workshops are available through the Center

- Cyberbullying and Cyberthreats – An introduction (1-1/2 hour presentation, with questions)
- Cyberbullying or Cyberthreat Situation Review and Intervention (3 hour interactive workshop)
- Comprehensive Approach to Address Cyberbullying and Cyberthreats (3 hour interactive workshop)

A limited number of personal presentation opportunities are available. Distance learning technologies are utilized by the Center to make the presentation and workshops available in any location with high speed Internet connectivity. The workshops are designed to facilitate a high degree of local interactivity, with the intention of contributing to the development of a solid local plan of action to address the concerns.. It is necessary for a needs assessment to be conducted prior to the Comprehensive Approach workshop.

The following book is under development:

- Cyberbullying and Cyberthreats.