Cyber-Safe Kids,
Cyber-Savvy Teens
Cyber-Secure Schools
Presentation Notes

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
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

Online Risks and Concerns
- Safety Risks
    – Young people victimized by others
- Responsible Use Concerns
    – Young people engaging in risky, inappropriate, harmful, or even illegal behavior
- Actually, more like a spectrum: Innocent - risky - inappropriate - harmful - illegal

Specific Risks and Concerns
- Sexually Related Risks
- Cyberbullying
- Unsafe Communities
- Dangerous Groups
- Cyberthreats
- Gaming Concerns
- Gambling
- Hacking
- Plagiarism
- Copyright
- Security Concerns
- Scams and Identity Theft
- Spam

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

Cyberbullying
- Online social aggression is being cruel to others by sending or posting harmful material or engaging in other forms of social aggression using the Internet or other digital technologies
  - Frequently, a continuation of or in retaliation for in-school bullying
  - Social aggression could also target school staff

Types of Cyberbullying
- Flaming
  - Online "fights" using electronic messages
- Harassment
  - Repeatedly sending offensive messages
- Denigration
  - Sending or posting material about a person to damage his or her reputation or friendships
- Impersonation
  - Posing as a person and posting material to make the person look bad, get 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 or tricking someone into revealing such information and then sharing
- Exclusion
  - Intentionally excluding someone from an online group
- Cyberstalking
  - Repeatedly sending threatening and intimidating messages or engaging in other online activities that make a person afraid for her or her safety

- Emotional harm may be greater than in-person bullying because …
  - Harm is on-going 24/7
  - Material can be widely disseminated and difficult or impossible to remove
  - Bully may be anonymous or may involve others
  - Teens are very reticent to tell adults about online concerns
  - Lack of knowledge of how to stop cyberbullying

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

Cyberthreats and Distress

- Posting or sending online material that is either a direct threat or distressing material that raises concerns that the person may be considering violence or self-harm
- May be tied to involvement in unsafe community or dangerous group
- Could be a joke, unsubstantiated rumor, impersonation, or real threat

Other Risks and Concerns

- Online Gaming
  - Excessive, addictive involvement in online games
  - Involvement in extremely violent games
- Online Gambling
  - Engaging in "gambling 101" game activities or actual online gambling
- Hacking
  - Breaking into or damaging computer systems
- Plagiarism
  - Inadvertently or intentionally using online information resources in an academically dishonest manner
- Copyright
  - Inappropriately copying, disseminating, or modifying someone copyrighted work
- Security Concerns
  - Accidentally infecting a computer with "malware"
- Scams and Identity Theft
  - Being deceived by an online scam, including theft of financial identity information
- Spam
  - Receiving excessive or highly inappropriate unwanted email messages

Foundational Issues

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

- 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

Addiction and Multitasking

- Media multitasking is attending to multiple tasks and multiple media
- Doing homework while media multi-tasking causes concern
  - Lack of ability to focus on important work projects
  - Likely major new cause of school failure

Information Literacy

- Anyone can post anything online
- Many individuals and groups are trying to influence the attitudes and behavior of others
- Many people judge accuracy of information based on appearance of the web site
- Assessing the accuracy of material online is an essential information age skill

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

Online "Place" Concerns

- Commercial Online Activities
- Social Networking Sites
- Chat Rooms and Groups
- Instant Messaging
- Cell Phones and PDAs

Commercial Online Activities

- Commercial web sites are actively engaged in market profiling and advertising
  - Encourage young people to disclose vast amounts of personal information
  - Promote unhealthy consumption, lifestyle, values, and behavior
  - Use specific strategies to enhance "stickiness," which can lead to addictive access
- Online marketing techniques include …
  - Advergaming - integrating advertisements into games or other entertainment
  - Permission marketing - encouraging children and teens to sign up to receive advertising
  - Viral marketing - encouraging children and teens to send marketing material to their peers
  - Social network marketing - a combination of advergaming, permission, and viral marketing

Social Networking Sites
- A place to express personal identity and maintain electronic connections with friends
- Concerns …
  – Disclose personal contact, provocative, intimate or reputation damaging material
  – Unsafe connections with dangerous individuals or groups
  – Engage in or are targeted by cyberbullying
  – Addictive access
  – Lie about their age to participate

Chat Rooms and Groups
- Chat rooms (real time) and discussion groups (not real time) provide the opportunity to communicate with others
  – The places where young people are most likely to meet online strangers
- Level of safety depends on …
  – Location or site
  – Subject under discussion
  – Whether there is a moderator

Instant Messaging
- Real time electronic communications using text or web cams
- Concerns …
  – Strangers can be included on "buddy" list
  – Inappropriate material, including sexual images, may be disseminated
- Level of safety depends on …
  – Who is included on the "buddy" list
  – Substance of material shared

Cell Phones and PDAs
- Emerging technologies that fit into a teen's back pocket can provide full online access
  – Which limits the ability of adults to effectively supervise their activities, especially in school
  – And means we have to empower them to independently make good choices

What is Not Working
- Filtering Follies
- Simplistic Rules
- Fear-Based Tactics
- Promoting Sole Reliance on Adults
- Avoiding Uncomfortable Information
- Considering that the Child is Always the Victim

Filtering Follies
- The misperception: "Filtering technologies will protect young people from harm as they surf the Internet"
  – Children's Internet Protection Act
  – Deleting Online Sexual Predators Act
    • Rep. Hastert: "(DOPA) would put filters in schools and libraries so that kids can be protected... We've all heard stories of children on some of these social Web sites meeting up with dangerous predators. This legislation adds another layer of protection."

- The reality:
  - Increased accidental exposure to pornography, despite increased use of filtering in the home
    - Crimes Against Children Research Center *Online Victimization* (2006)
  - Top selling filtering products had a 10% failure rate in blocking intentional access to pornography
    - Kaiser Family Foundation *See No Evil* (2002)
  - It is easy to bypass filters using various proxy technologies - Google: "bypass Internet filter"
- (The report, *Youth, Pornography, and the Internet,*) will disappoint those who expect a technological "quick fix" to the challenge of pornography on the Internet. … It will disappoint parents, school officials, and librarians who seek surrogates to fulfill the responsibilities of training and supervision needed to truly protect children from inappropriate sexual materials on the Internet.
    - U.S. National Academy of Sciences, Dick Thornburgh, chairman (2002)

Simplistic Rules
- An example: "Don't post personal information online"
  - How do I register on a site?
  - How do I purchase something on E-bay without providing my name and address?
  - I have a username, so it is okay to post pictures of myself in a bikini. Right?
  - How can I have fun on MySpace without sharing information about who I am?

Fear-Based Tactics
- Online Stranger = Danger!
  - "We … were stunned to learn the vast numbers of teens engaging in <u>incredibly</u> risky behaviors online." (emphasis added)
  - "Half of teens 13-18 have communicated online with someone they have never met.
  - One third have talked about meeting in person someone they only know online."
    - Paula Klaas Foundation (2006)
- Frequently, Internet safety education communicates that it is "highly likely" …
  - That online strangers will pretend to be someone they are not
  - That online strangers are very dangerous
  - That if a young person meets in person with someone they met online, that stranger will try to harm them
- The Reality:
  - "Stranger-danger" warnings are not effective at keeping kids safe
    - National Center for Missing and Exploited Children
  - Adolescent risk prevention research has demonstrated that fear-based prevention approaches are ineffective
  - Many teens communicate with online strangers and will meet in person with online strangers - the vast majority of whom are perfectly safe
- Fear-based messages communicate that "Adults don't get it"
  - Teens know that adults are afraid of new technologies
  - They simply dismiss fear-based messages as evidence that adults are afraid of what they do not understand
  - AND they are less willing to come to an adult for help when they really should because they think adults will overreact!

Sole Reliance on Adults

- Standard Internet safety message: "If you feel uncomfortable about something that happens online, tell an adult."
- Teens are not going to tell adults about online concerns if they think that adults will overreact, blame them, restrict their online access, not know what to do, or make the problem worse!
  – Teens need assurance that adults will know how to effectively respond and will not overreact or make matters worse

Uncomfortable Information

- Two leading Internet safety education programs for middle school students …
  – Do not use the word "sex"
  – Do not discuss the sexual intentions of predators
  – Do not address why these sexual relationships are unhealthy and dangerous
- If adults are too scared to talk about risky sex with teens, then how do we expect teens to be comfortable reporting that someone is "hitting on them" online?

Child is Always the Victim

- FBI *A Parent's Guide to Internet Safety:* "Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions."

- This is legally accurate, but …
  – Teens are posting sexual provocative images, using sexually inviting usernames, and engaging in online activities for the purpose of "hooking up"

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

- Children simply do not have the cognitive development to engage in effective and safe online decision-making
- In teens, the frontal cortex is undergoing significant development
  – Frontal cortex supports rational, ethical decision-making
  – Learning to make good decisions requires practice and attention to actions and consequences
- Teens process emotions in the "flight or flight" region of brain
  – So if emotions are involved (and when are they not?) teens are less able to make good choices
- When online …
  – There is an interference in recognizing 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 and 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

- Public exploration of identity can lead to disclosure of highly intimate or reputation damaging material
- Number of links and amount of communication activity is new measure of social status and self-worth
  – High social anxiety fuels addictive access and bad attention-getting choices
- Cyberbullying is closely tied to social status concerns
- Exploring emerging sexuality
  – In a society where entertainment, advertising, clothing promotes provocative sexuality
  – And in an online environment that frequently includes young adults and promotes provocative sexuality and "swinging"
    • Sexually provocative online advertisements
    • Advertisements for match-making sites
    • Activities such as "hot or not?" contests
    • Profile questions about sexual interests and activities

Online Social Norms

- "Everybody does it"
- "Life online is just a game"
- "Look at me—I'm a star"
- "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
  – Reciprocity
    • Provide a gift (tangible or intangible) and this creates a feeling of indebtedness - predators use excessive complements and provide gifts
  – Seek a commitment
    • Supports attitudes and behaviors that are consistent with the commitment - commercial advertisers seek commitment to their product or services
  – Group think
    • Go along with what the group thinks or does - unsafe communities or dangerous groups encourage group allegiance
  – Attractiveness, similarity, and familiarity
    • Comply with requests from people who are known and liked- people "image manage" online
  – Establish position of authority
    • Respect and obey people in a position of authority - commercial web sites, predators, recruiters establish authority
  – Threat of scarcity
    • Act now or you will lose - used by scammers

Protecting Children

- Children do not have the cognitive capacity or experience to independently make good choices online
- All use should be in a controlled environment
  - Book-marked sites
  - Closely controlled communications
  - Close supervision
- Three simple rules for children
  - Do not go outside of the previewed sites without permission
  - Do not type your name, address, or phone number online
  - If something "yucky" appears, turn off the screen and tell an adult

Teen Online Risk

- Teen online risk must be viewed from perspective of adolescent risk
- Savvy … Naïve … Vulnerable … At Risk
- Savvy teens have effective knowledge, skills, and values to make good decisions
  - Likely to be older teens, with healthy peer relationships, and attentive parents who have fostered independence and personal responsibility
- Naïve teens lack sufficient knowledge and skills to engage in effective decision-making
  - Likely to be younger teens, have either over protective or naïve parents, but likely have healthy peer relations and good values - can become savvy teens
- Vulnerable teens lack the necessary knowledge and skills and are also are going through a period of "teen angst"
  - Likely to have temporarily impaired relations with parents and/or peers
- At risk teens are those who are "at risk" in other areas of life
  - Face major ongoing challenges related to personal mental health and disruptions in relations with parents, school, and/or peers

Online Risk Factors

- The higher the degree of risk, the greater the probability the teen will be …
  - Searching for acceptance and attention from people online
  - More vulnerable to manipulative influence techniques used by dangerous individuals and groups
  - Functioning in "fight or flight" mode and thus less likely to make good choices because they are not "thinking clearly"
  - Less attentive to Internet safety messages
  - Less resilient in getting out of a difficult situation even if he or she wants to
  - Less able or willing to rely on parents for assistance
  - Less likely to report an online dangerous situation to an adult because this will likely 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 teens to provide guidance and assistance to peers and report online concerns to adults

Four Key Strategies
- Address privacy concerns
- Prevent Internet addiction
- Enhance information literacy
- Ensure stranger literacy

None of Your Business
- Personal Contact and Financial Information
  - Should only be disclosed by older teens on secure sites for an appropriate reason
- Intimate Information
  - Should never be disclosed publicly
  - May be disclosed privately with very trustworthy friends or on a professional social support site.
- Reputation Damaging Material
  - Should never be disclosed online
- Sensitive Personal Information About Others
  - Should never be disclosed online

Keeping Life in Balance
- Parent involvement is likely necessary
- Teens can be taught …
  - The importance of maintaining balance in their life activities
  - That media-multitasking while doing homework can significantly interfere with effective learning

Don't Take Candy From Strangers
- Children and tweens should not communicate with online strangers
- Teens must learn to determine the safety and trustworthiness of an online stranger
- And how to meet with this person safely, if there is a desire to do so

Stranger Guidelines
- Use your values to guide your assessment of strangers online
- Reflect on how you met this person
- Carefully review the person's online presence — material posted, friends, and communications
- Take time to get to know people online. It is hard to keep a facade
- Pay attention to details of messages and watch for inconsistencies
- Ask others for their opinion

RED FLAGS!
- Watch out for anyone, especially an adult, who sends "overly-friendly" messages, offers gifts, tries to establish a "secret" relationship, asks for a sexy picture, or tries to turn you against your parents or friends!

Safe Meeting Guidelines
- NEVER agree to meet with an online stranger without parent approval of a safe meeting plan
- Any meeting should be in a public place, with parent or trusted friends nearby
- Pre-arrange a safety check phone call with a parent 5 minutes into the meeting
- Never leave the public place with the online stranger

Read With Your Eyes Open
- Consider how important it is that the information be credible
- Assess how controversial the issue is, because this could affect bias
- Reflect on how you got to a site or received the information
- Evaluate the source of the information looking for potential bias and what the source is seeking or has to gain if you agree with their information or position
- Determine whether the information is fact-based or opinion-based
- Determine whether the information is consistent with information found through other sources
- Ask for the opinions of others, especially a parent, teacher, or librarian
- Evaluate the information itself

Specific Safety Risks
- Sexual Predators
- Accidental Access of Pornography
- Cyberbullying
- Scams

Sexual Predators
- Follow the stranger literacy guidelines and watch out for "red flag" messages
- Posting sexually provocative material, joining groups to discuss sex, or sharing intimate personal information is likely to attract a predator
- Recognize …
  - Sexual predators are not "lovers" or "mentors" — they are abusers and losers
  - Meeting with a sexual predator could result in sexually transmitted disease, forced engagement in risky sex, abduction, and murder
- Save all evidence of any contact by a possible predator and report
- Friends don't let friends hook up with online predators

Accidental Access
- Don't click on a link, if you do not know what it will access
- Don't type a URL - type the name of the site in a search engine
- Don't open suspicious email messages
- Don't download peer-to-peer networking software
- Use a browser that blocks pop-up ads

Cyberbullying
- Don't post or send information that others could use against you
- Don't Retaliate!
  - This only gives the bully a "win" and makes you part of the problem
- Save the evidence and seek to determine the identity of the aggressor
- Response options …
  - Calmly and strongly tell the person to stop or you will take further action
  - Ignore or block the communications
  - Communicate with the parents of the aggressor
  - File a complaint with the site, ISP, or cell phone company
  - Seek assistance from school officials

– Contact an attorney
– Contact law enforcement

Scams

- Be very wary of any opportunities that are "too good to be true" or warn "act now or you will lose out"
- These are key indicators of a scam

Good Choices Online

- Compare family values, school Internet policies, web site terms of use agreements, and civil and criminal law standards
  – They all express similar standards
- To make good choices online, ask …
  – "Is this kind and respectful to others?"
  – "How would I feel if someone did or said the same thing to me, or to my best friend?
  – "What would my mom, dad, or other trusted adult think or do?"
  – "Would I violate any agreements, rules, or laws?
  – "How would I feel if my actions were reported on the front page of a newspaper?"
  – "What would happen if everybody did this?"
  – "Would it be okay if I did this in Real Life?
  – "How would this reflect on me?"

Legal Issues for Schools

- Privacy (search and seizure)
  – Internet use through district Internet system
  – Personal digital devices
- Free Speech
  – Student access to information
  – Student speech through district Internet system
  – Student speech off campus
- School Liability

Privacy

- Student privacy rights when using Internet in school are similar to "locker search"
  – Students should expect general monitoring of online activity by staff or technically
  – Individual searches may be conducted if there is a reasonable suspicion of misuse
- Legal concerns related to review of personal digital devices (cell phones, PDAs)
  – Appears to be a violation of wiretapping law

Access to Information

- Students should not be prevented from accessing educationally appropriate material based on viewpoint discrimination
  – Many filtering products are blocking access based on viewpoint discrimination, especially to materials related to safe sex, sexual orientation, and non-traditional religion
- Selected school staff should have the ability to temporarily override the filter to review a blocked site and provide student access, if deemed appropriate

Student Speech

- Schools have the right to apply educationally based restrictions to student speech through the district Internet system

- Schools may apply formal discipline for off-campus speech only if the speech causes a substantial and material disruption at school, or threatens such disruption

School Liability
- Liability concerns are raised when students may be harmed through actions that are occurring through district Internet system
  – Cyberbullying, including sexual or racial harassment
  – Communications with predator
  – Participating in an unsafe community
  – Planning school attack
  – …
- Negligence Liability
  – Schools have a duty to anticipate foreseeable dangers and to take necessary precautions to protect students
  – A breach of this duty occurs when a school official fails to exercise a reasonable standard of care in the context of a foreseeable risk
  – If a student's injury should have been foreseen and could have been prevented through the exercise of reasonable precautions and an injury has resulted, the school can be held liable
- Civil Rights Statutory Liability
  – 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 is established if upon reasonably diligent inquiry school officials should have known of the discrimination

Internet Use Management
- Significant concerns about the effective management of Internet use in schools
  – Filtering is ineffective and can easily be bypassed
  – Policies generally have not been updated to reflect new concerns
  – Teachers have not received sufficient professional development
  – Internet activities have not been effectively integrated into the curriculum
  – Far too much "Internet recess" occurring in schools - Internet use for entertainment not education
  – Youth risk online must be addressed from the perspective of adolescent risk
    • But safe school personnel do not understand the Internet and are not involved in making Internet use management decisions
    • And educational technology personnel do not have an effective understanding of adolescent risk concerns
- Foundation of an effective approach …
  – Limit non-educational use of the Internet
  – Protect elementary students
  – Educate and hold middle and high school students accountable
  – Implement effective supervision and monitoring practices

Education Purpose
- Internet use in schools should generally be for educational purposes only
  – Classwork and independent research on subjects similar to what is studied in school or resources in the school library
  – Necessary preparation for workplace where Internet use is restricted to work activities

- Schools may establish or allow limited opportunities for entertainment use
  – But specific parent permission should be obtained
- Increased professional and curriculum development is an essential foundation
- Clear expectations for teachers: "Internet recess" is not an appropriate educational activity during class instruction time
  – Also need clear standards for substitutes
- Restricting "Internet recess" will be difficult in some schools because free use is expected - by students and teachers

Internet Use Policies
- Reviewed regularly to address new concerns
- Clearly tied to disciplinary code
- Clearly communicated to staff and students
- Provide foundation for student education

Internet Use Practices
- Previewed educational sites
  – Previewed research resources or teacher previewed sites
- Controlled communications facilities
- Allow research outside of previewed educational sites for specific projects at middle and high school level
  – Use as opportunity to teach information literacy
- Provide access to reviewed sites for sensitive health information

Effective Monitoring
- Must shift from "blocking" approach to effective monitoring
- Monitoring must be sufficient to detect most instances of misuse
- Teacher supervision and frequent request to view history file is essential
- Technology-facilitated monitoring is strongly advised
  – Real time or intelligent content analysis

Comprehensive Approach
- Coordination
  – Youth risk online is a safe schools issue and thus Internet use management should fall under the jurisdiction of the safe schools committee with the addition of educational technology personnel
- Policies and Practices
  – Must be regularly reviewed and updated
- Professional Development
  – School staff should have sufficient knowledge of youth risk online issues, as required by their position and job responsibilities
- Student Education
  – Simple rules education for children
  – Overall safe and responsible Internet use education for middle and high school students
  – Specific education related to instructional activities
- Parent Outreach
  – Many of the concerns related to student Internet use are originating at home

- Schools should provide outreach to parents
  - Workshops, newsletter material, resources at school
- Community Outreach
  - The district should have a coordinated approach with law enforcement and social service organizations to address youth risk online concerns
  - Community organizations can provide an additional vehicle for parent outreach
- Continuous Improvement
  - Ongoing assessment and evaluation can support continuous improvement
    - Technologies are changing
    - Online activities are changing
    - Research about risk issues is emerging
    - Legal issues are not yet fully clarified

Reprise
- To effectively address Internet risks and concerns it is necessary to …
  - Keep younger children in safer places and teach them simply safety rules
  - Empower teens with the knowledge, skills, and values to make good choices
  - And to remain engaged to ensure they do.

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).