Cyber Savvy Teachers

Digital Media Safety and Citizenship

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Internet Use

Preface: Teach Them to Swim

Teach Them to Swim

"*Swimming pools can be dangerous for children. To protect them, one can install locks, put up fences, and deploy pool alarms. All of these measures are helpful, but by far the most important thing that one can do for one's children is to teach them to swim.*"[1]

- It is impossible to effectively teach students to swim if ...
  - They can't jump into a swimming pool while at school because it is considered too risky.
  - Their teachers only know how to paddle in the shallow part of the pool or are afraid to get wet.
  - Despite the fact that they have grown up in the water and most have excellent swimming skills, they are constantly warned that water is dangerous and filled with sharks.

Cyber Savvy Schools Vision

- Cyber Savvy Schools know that the digital media revolution has changed society. Cyber Savvy Schools know they must effectively prepare students to engage in safe and responsible behavior ~ and to use these technologies effectively for the betterment of themselves and our global society.

21st Century Learning Environments Enriched with Web 2.0 Technologies

- Schools are effectively using Web 2.0 technologies in the context of enriched 21st Century learning environments to prepare students for their future education and careers, civic responsibilities, and personal life in the 21st Century.

Universal Digital Media Safety, Citizenship, and Literacy Competencies[2]

- All young people understand digital media safety, citizenship, and literacy issues and demonstrate competence in ...
  - Keeping themselves safe.
  - Engaging in responsible behavior that respects the rights of others.
  - Taking responsibility for the well-being of others.
  - Effectively consuming, creating,, contributing, and communicating in a digital media environment.

Targeted Youth Risk Online Prevention and Intervention

- Effective risk prevention and intervention programs have been established to respond to the concerns of the minority of young people who are at greater risk of engaging in unsafe or irresponsible online behavior or being victimized by others.

Presentations by the Center for Safe and Responsible Internet Use

- All of the presentations provided by the Center for Safe and Responsible Internet Use are directed at one of these three issues. This presentation is focused on ensuring students gain universal digital media safety, citizenship, and literacy competencies.

---

1 Thornbourgh, D, & Lin, H. (2002) *Youth, Pornography and the Internet.* National Research Council, http://www.nap.edu/openbook.php?isbn=0309082749.

2 Note: The terms "digital media" and "online" include both Internet use and use of other digital devices, including cell phone.

About This Presentation

Part I ~ Instructional Insight

- Overview of Issues and Concerns.
- Influences on Online Behavior.
- Instructional Strategies
- Guidance for Parents.
- School Staff Online.

Part II ~ Internet Safety Education

- Cyber Safe Kids ~ Primary
- Cyber Savvy Kids & Teens ~ Intermediate, Middle and High School
- Foundational Issues
  - Making good choices.
  - Addictive access.
  - Posting personal information.
  - Interacting with others.
- Sites and Technologies
  - Computer security and scams.
  - Acceptable use agreements.
  - Online pornography.
  - Market profiling and advertising.
  - Social networking.
- Specific Risks
  - Electronic aggression.
  - Risky sexual and personal relationships.

Appendix

- Recommended lesson plans.

Note

- While CSRIU has provided handouts for students addressing these issues which can be used to support instruction, the information provided in this presentation will provide the insight necessary to use other Internet safety curriculum ~ if that curriculum is grounded in current research understandings and effective risk prevention.

Not Included

- What this presentation does not cover are an entire set of issues related to Digital Media Literacy. This includes: information credibility, influence techniques, free speech, accurate attribution, copyright, publisher responsibilities, establishing credibility, effective advocacy and civic collaboration. These issues will be addressed in forthcoming materials.
- More information on the higher level risks is available in another CSRUI presentation entitled: *Youth Risk Online: A Guide for Professionals Who Work with Children and Teens*.

Part I ~ Instructional Insight

Overview of Issues and Concerns

Raising Kids in the Real World

- When children are young, we keep them in safe places, like fenced play yards. As they grow, we ensure they understand the risks and effective protective strategies. And we remain engaged.
- Applied to cyberspace:
  - Children should use the Internet in protected places.
  - Teens must know how to make safe and responsible choices online.
  - Adults must remain actively and positively engaged.

Digital Divide Challenge

- Young people are cruising down the Information superhighway with their accelerators fully engaged but sometimes without sufficient braking power, while most adults are struggling to get out of first gear.

- They still need adults!
  - Research has shown that children whose parents are **actively** and **positively** involved engage in far less risk-taking behavior online.
- But many are not listening to adults.
  - Young people know that many adults do not understand ~ and some fear ~ their new wonderful online world.
- Fear-based messages about the Internet are:
  - **Not** causing parents to become engaged.
  - Causing teens to **not** trust adults.

Change in Paradigms

- Old paradigm.
  - Adults understood the risks and the environment.
  - Adults were generally in a position to detect risky behavior and intervene.
  - Adults were the authority.
- New Paradigm.
  - Adults are the "digital immigrants." Although we can accommodate, we will never fully acculturate.
  - Teens are often participating in environments where there is no adult supervision.
  - Adults who pretend to be authorities will lead teens to ROFL (roll on the floor laughing).

School Systemic Divide Challenge

- Frequently, educational technology staff are assigned the responsibility of teaching Internet safety.
  - They understand the technologies and digital culture, but they often don't understand risk prevention.
- Library media specialists have the greatest insight into media literacy, which is an important foundation for all aspects of safe, ethical, and responsible online behavior.
  - But they also often don't understand risk prevention.
- Counselors and health education teachers understand youth risk prevention.
  - But they often don't understand the technologies and digital culture.
- All areas of expertise are essential!

Techno-Panic

- Techno-Panic is stopping the conversation!
  - Techno-Panic is a heightened level of concern about the use of contemporary technologies by young people that is disproportionate to the empirical data on the actual degree of risk.
  - We must neither ignore nor exaggerate the risks. We must have an accurate understanding of the risks.

What the Research Says[3]

- The young people who are at greater risk online are the ones who are at greater risk in the Real World.
- Young people face greater risks from known peers than from online strangers.
- The majority of young people are generally making good choices and effectively handling negative incidents.
  - But they are young. They make mistakes. They test boundaries. They are influenced by others. They do not recognize the risks.

Fear of Overreaction ~ and They "Fixed It"

- Young people often don't tell adults about online concerns because they fear adults will overreact, blame them, not know what to do, make things worse, restrict their online access.
  - But also, many times teens don't tell because they have already fixed the problem.
  - It is developmentally inappropriate for teens to always tell adults about online problems. An important life task in the teen years is learning how to take care of your own problems.
  - We need to empower and trust them.

New Risks?

- These are not new risks. This is just a new environment for common risks faced by young people. But this is an environment where ...
  - They can be invisible or highly public.
  - What they post can remain publicly and permanently accessible.
  - Whey receive less tangible feedback about the consequences of their actions and may be deceived by others.
  - They may be functioning with much larger groups of people, including those who are unknown in the real world.

---

3 In January 2009. the Berkman Internet Safety Technical Task Force released a report on concerns of youth risk online. A companion report was prepared that provided a comprehensive overview of all of the research in this area. cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_C_TF_Project_Plan.pdf.

- Responsible adults may be less present.

✦ So it appears that risks are greater in this environment

Cyber-Savvy

Savvy

✦ From Latin *sapere* to be wise. Astute, well-informed, capable, perceptive, intelligent, discerning.

Keep Themselves Safe

- They understand the risks. They know how to prevent themselves from getting into risky situations, detect if they are at risk, and effectively respond, including asking for help.

Do the Right Things

- They do not harm others. They respect the rights, privacy, and property of others.

Take Responsibility for the Well-being of Others

- They help others online. They report concerns to a responsible adult or site.

Good Choice ~ Bad Choice

Influences on Online Behavior[4]

You Can't See Me

✦ Perception of invisibility or ability to be anonymous. Reduces concerns about detection, disapproval, or punishment.

✓ Encourage them to make choices based on internalized values and recognize they are not truly invisible, especially in Web 2.0 environments.

I Can't See You

✦ No tangible feedback about consequences of online activities. Can interfere with recognition of harm and feelings of empathy and remorse. Can also interfere with the ability to detect when others are being deceptive.

✓ Focus their attention on harmful consequences and the importance of not trusting everything they are told online.

Didn't Think

✦ Children's brains are insufficiently developed to fully comprehend the Internet. If they still believe in the tooth fairy, they can't comprehend the Internet. It is a magic box.

✓ Protect children and provide easy to follow guidelines.

✦ Teen's brains developing the capacity for effective decision-making. They are biologically incapable of consistently thinking clearly ~ but biologically compelled to make their own decisions. And they want to resolve problems on their own.

✓ Teach them how to engage in effective, independent problem-solving and effectively resolve negative situations.

Who Am I?

✦ Teens online activities allow them to explore their personal identity. May lead to inappropriate postings or activities.

✓ Encourage them to pay attention to their online "image" and reputation.

Am I Hot?

✦ Exploration of emerging sexuality and relationships. Can result in posting provocative images and "fantasy love."

✓ Honestly discuss issues of sexuality and relationship risks online.

If I Can Do It, It Must be OK

✦ The easy ability to do something creates the perception that it is permissible.

✓ Tell them, "Just because you can, doesn't make it right."

Everybody Does It

✦ They may follow others who make inappropriate choices. Watch out for "friends."

---

4 These issues are discussed in more depth in: Willard, N. (2004) I Can't See You – You Can't See Me: How the Use of Information and Communication Technologies Can Impact Responsible Behavior. http://csriu.org/documents/disinhibition.pdf.

✓ Tell them, “Just because they do it, doesn’t make it right.”

How Far Can I Go?

✦ Teens test boundaries because this how they learn about boundaries.

✓ Help them understand why there are limits. There are limits because if you engage in certain behavior this can cause harm to self or others.

Doing What They Say

✦ Others seek to manipulate them. Offer “online **candy**” ~ complements, gifts, opportunities. Or they encourage **commitment** to special relationship or a group.

✓ Teach them to recognize attempted manipulation.

Looking for Love

✦ Teens who face Real World personal challenges are at higher risk online: More likely to look for attention. More vulnerable to manipulation. Less likely to recognize obvious risks. Less likely to make good choices. Less likely to report concerns ~ because more likely to have engaged in risky behavior.

✓ School staff involved in safe schools/health and educational technology staff must collaborate to address the more significant risks faced by a minority of young people online.

✦ Other teens are in the best position to detect these concerns.

✓ Encourage more savvy youth to assist their peers and report online concerns to adults

---

Instructional Strategies

Effective Education & Risk Prevention

Instructional Objectives

✦ The instructional objectives that will be set forth to address each risk area below are grounded in the following overall objectives that are associated with the National Health Education Standards, the National Educational Technology Standards, and Information Literacy Standards. In the following section, the initial standard is the original standard The indented standard is the application to online issues.

National Health Education Standards

Source: Center for Disease Control School Health Education Resources.[5]

1. Students will comprehend concepts related to health promotion and disease prevention to enhance health.
   - Students will comprehend concepts related to online risks to their health and well-being. ,
2. Students will analyze the influence of family, peers, culture, media, technology and other factors on health behaviors.
   - Students will analyze how interactive technologies, online peers and adults, online media and advertisers, and manipulation techniques used online can influence their attitudes and behavior related to health and well-being.
3. Students will demonstrate the ability to access valid information and products and services to enhance health.
   - Students will demonstrate effective assessment of credibility of resources found online and the ability to access online information, support and referral services related to health and well-being.
4. Students will demonstrate the ability to use interpersonal communication skills to enhance health and avoid or reduce health risks.
   - Students will demonstrate the ability to use electronic communication technologies to engage in refusal, negotiation, dispute resolution, request for assistance, and provision of assistance to others.
5. Students will demonstrate the ability to use decision-making skills to enhance health.
   - Students will understand negative influences on online behavior and engage in effective problem-solving and decision-making in relation to online influences on online and offline behaviors that impact health and well-being.
6. Students will demonstrate the ability to use goal-setting skills to enhance health.

---

5 http://www.cdc.gov/healthyyouth/sher/standards/index.htm.

- Students will demonstrate the ability to use goal-setting to prevent online risk, engage in ethical online behavior, and demonstrate responsibility for the well-being of others online.

National Educational Technology Standards for Students

Source: International Society for Technology in Education.[6]

4. Critical Thinking, Problem Solving, and Decision Making. Students use critical thinking skills to plan and conduct research, manage projects, solve problems, and make informed decisions using appropriate digital tools and resources.
   - Students will: identify online risk situations, engage in effective problem-solving to respond to risk situations, and make informed, ethical decisions regarding personal online behavior.
5. Digital Citizenship. Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior.
   - Students will: advocate and practice safe, legal, and responsible use of information and technology; practice effective online collaboration; demonstrate personal responsibility for the well-being of others; and exhibit leadership for digital citizenship.

Information Literacy Standards

Source: American Association of School Librarians[7]

2. Draw conclusions, make informed decisions, apply knowledge to new situations, and create new knowledge.
   - Students will evaluate the information posted or provided by others online to determine the credibility of the information posted and the safety of the person communicating such information.
3. Share knowledge and participate ethically and productively as members of our democratic society.
   - Students will do the right things and take responsibility for the well-being of others.
4. The student who contributes positively to the learning community and to society is information literate and practices ethical behavior in regard to information and information technology.
   - Students will engage in ethical behavior with respect to their online activities, including the information they post and their use of information posted by others.

Scope and Sequence

✦ It must be recognized that by the time young people turn 13 they are essentially considered to be fully capable of engaging in most online activities, other than those specifically limited to "adults." Many young people are lying about their age and entering the general cyberworld around age 10. There are continuing reports of incidents involve risky online actions of 4th and 5th grade students. Thus, by early middle school, young people need to be prepared to handle all of the safety concerns set forth below.

✓ Provide simple rules for primary grade students.

✓ Introduce core protections in intermediate grades.

✓ Expand on core principles in middle school, especially with an expanded focus on the risky sexual and personal relationship concerns.

✓ Focus in high school is on preparation for adult use and full participation in a digital world ~ thus a strong focus on the Digital Media Literacy issues.

Student Instruction ~ How & When

✓ Provide direct instruction.

- Review of Internet use policy. Technology or library class. Health classes ~ address youth risk issues. Student homerooms or advisories.

✓ Integrate into other instruction.

- Especially Web 2.0 instruction.

✓ Use teachable moments.

- Use incidents and news stories as opportunities to focus on Real World consequences. Especially appropriate activities for home rooms or student advisories.

✓ Provide informal instruction.

- Signs in the computer lab, brief hints on the computer screen, and the like.

Parent Instruction ~ How & When

✦ Schools are an important conduit of Internet safety education for parents. The following approaches can be used:

✓ Host parent workshops.

✓ Provide resources in office and library.

---

6 www.iste.org/NETS/.

7 Information Literacy Standards for Student Learning. http://www.ala.org/ala/mgrps/divs/aasl/aaslissues/aaslinfolit/informationliteracy1.cfm.

- ✓ Publish information in newsletters and on district/school web sites.
- ✓ Provide information tied to student instruction.

✦ Unfortunately, the parents who are likely most in need of the insight and information frequently are the parents who are least likely to pay attention.

- ‣ But the engaged parents who will pay attention also are most likely to have children who can be important peer leaders. Focus attention on how parents can encourage their children to assist others or report online concerns.

21st Century Learning

✦ Schools cannot effectively prepare students for their future education, careers, personal life, and civic responsibilities without embracing Web 2.0 technologies.

- ‣ Support exciting, relevant, interactive instruction and learning ~ but present management challenges.

Current Challenges

✦ Concerns about the safety of students, largely based on inaccurate information about online sexual predators, is leading to unjustified restrictions on student Internet use at school.

✦ Primary reliance on ineffective filtering.

- ‣ Students can often bypass the filter. Filter is blocking appropriate educational resources.

✦ Insufficient professional and curriculum development.

✦ Lack of technologies and strategies to effectively manage interactive instruction.

Effective Approach

✦ Focus on use of digital media resources and technologies to facilitate learning where appropriate in the curriculum.

- ‣ Fully integrate the district's educational technology program into Curriculum and Instruction.
- ‣ Establish a Web 2.0 professional community to support ongoing dialogue, sharing of lesson plans, and mentoring.
- ‣ Expand role of library media specialists to that of digital media literacy specialists ~ professionals who support teachers and students in gaining digital media literacy.
- ‣ Adopt a "continuous improvement" model to support innovative approaches with effective evaluation.

✦ Revise approach for technology use management.

- ‣ Reinforce that the Internet must be used for learning activities, not entertainment. Periodically analyze technology use to ensure instructional focus.
- ‣ Shift from primary reliance on "blocking" to more effective "watching" ~ through use of remote access or content analysis technical monitoring and staff supervision.
- ‣ Implement a district Web 2.0 interactive environment for professional development and student use.
  - Blogs and wiki environments that are easy for teachers to manage and are not publicly accessiblr.
  - Provide students with an online "classwork portfolio," accessible through the Internet from any device or location ~ with the ability to email work to a teacher or post work to a blog or wiki for group collaboration.
  - Provide web-based lesson development and white list capabilities for teachers.
- ‣ Establish two levels of blocking and overriding authority.
  - "Harmful categories" that require approval to override.
  - "Management categories" that can be overridden by any teacher for instructional purposes or to address safe schools concerns. Establish clear standards that address purpose, content, and bandwidth concerns. Overriding is recorded which will ensure accountability.
- ‣ Establish student "tech teams" to provide computer trouble-shooting and support in the use of technologies.

Social Norms Risk Prevention

✦ The National Social Norms Institute provides excellent guidance.[8] The following is from their FAQ:

> Until recently, the predominant approach in the field of health promotion sought to motivate behavior change by highlighting risk. Sometimes called "the scare tactic approach" or "health terrorism," this method

8 http://www.socialnorms.org.

essentially hopes to frighten individuals into positive change by insisting on the negative consequences of certain behaviors.

This kind of traditional strategy has not changed behavior one percent.

Essentially, the social norms approach uses a variety of methods to correct negative misperceptions [usually overestimations of (risky behavior)], and to identify, model, and promote the healthy, protective behaviors that are the actual norm in a given population. When properly conducted, it is an evidence-based, data-driven process, and a very cost-effective method of achieving large-scale positive results.

✦ Use a social norms approach.

- Correct misperception that other teens are engaging in risky online behavior. If they know other teens are not engaging in risky behavior they are much less likely to do so either. Identify, model, and promote the healthy, protective behaviors that are the actual norm in a given population.

Normative Online Behavior

✦ National research demonstrates the majority of young people are generally making good choices online and responding effectively to the negative incidents that occur.

- Reinforce this.

Risk Factors ~"Online Traps"

✦ The above discussion of influences on online behavior outlines the key risk factors. In student materials, these have been simplified are are referred to as "online traps."

- Perception of invisibility.
- Lack of tangible feedback about negative consequences or deception.
- Acting fast and not thinking ~ combined with the potential for material posted electronically to become public and permanent.
- Negative influences of others in online communities ~ especially manipulation used by others online and communities of others who are "at risk."
- Easy to engage in certain harmful activities.
- "At risk" youth engaging in risky behavior online.

Protective Factors

✦ The key protective factors appear to include:

- The majority of teens have no desire to be victimized online or do things that will damage their reputation, social standing, or future opportunities.
- In Web 10 environments, people could be invisible. But in Web 2.0 environments, there is significant visibility.
  - Stated otherwise: On Web 1.0, no one knew you were a dog[9] On Web 2.0, not only do they know you are a dog, they know what breed you are, who you run with, where your bones are buried, the accidental piddle behind the couch, the fight you got into with the boxer, and your thoughts on the hot poodle down the street.

Social Intelligence

✦ All of the issues of concerning online behavior are related to underlying problems some young people have in handling personal and social interactions ~ the domain of social intelligence.

- Social intelligence is as important as performance in language arts and mathematics.

✦ The foundation for addressing Internet safety and youth risk online is helping students gain effective social and personal relationship understandings and skills.

- Positive behavior support, development of empathy, interpersonal problem-solving, and peer mediation must be comprehensively addressed in every school.

Reefer Madness ~ Just Say "No"

✦ This section addresses approaches to avoid and alternatives to use when providing Internet safety instruction.

Inaccurate Information

✦ Much of the messaging around the prevalence and behavior of online predators is inaccurate. These incidents are largely under the control of teens if they use protection measures on social networking sites and stay out of chat rooms that attract adults. Inaccurate information about other online risks is also sometimes presented.

✓ Provide accurate information. Require any provider of Internet safety curriculum to demonstrate how their information is supported by academically published research.

No Fear-Based Messages

✦ Teens dismiss Internet "fear" messages as an adult overreaction and lack of understanding. Increases the probability tens will not listen or report concerns. Also this does not increase positive parent involvement.

✓ Provide practical information about risks and protective strategies.

---

9 From a famous cartoon by Peter Steiner, *The New Yorker*, July 5, 1993.

No Stranger-Danger Warnings

- ✦ Stranger danger warnings do not work in the Real World and will not work online. Online incidents involving known peers are far more harmful and difficult to address. Most strangers are perfectly safe ~ but because it is not possible to check them out in the Real World require greater caution.
  - ✓ Help students learn how to interact safety with people they know in person and those they meet or get to know online.

Not "Just Say 'No'"

- ✦ Simplistic rules against normative online behavior will not work. Young people will post material online and interact with people they do not know.
  - ✓ Provide simple guidelines for children. Provide teens with comprehensive insight on how to prevent and effectively respond to online concerns.

Not Sole Reliance on Adults

- ✦ Teens will not tell adults about online concerns simply because we tell them to. For children, it is appropriate to advise them to tell an adult. Teens want to resolve problems on their own ~ and developmentally this is what they need to do.
  - ✓ Teach teens how to effectively respond to most incidents. Tell them what adults can do to help if there is a significant or unresolved concern. Make sure they know that even adults sometimes have to ask for help. Encourage them to assist peers and report significant concerns to adults.

Don't Act Like an Authority

- ✦ Teens do not believe that adults understand their digital world as well as they do ~ and in most cases they are correct. In other words, "Never try to act like a sage on the stage ~ you will likely trip on your toga."
  - ‣ You can, however, act like an authority with elementary students.
  - ✓ Respect their insight. Set up situations where savvier students communicate guidance to peers and you can ask guiding questions to lead to deep understanding. Use older students to teach younger students.

No Techie Quick-Fixes

- ✦ A techie "quick fix" is an ineffective technology that seeks to control the behavior of teens. It is impossible to keep teens in electronically fenced play yards. There are effective technology protections for children.
  - ✓ Encourage parents to use technical protections for children.
  - ✓ Encourage teens to use the protective features of sites.

Evaluating Curriculum

- ✦ While CSRIU has prepared student handouts that can be used to support instruction with students, this presentation has been designed to provide educators with the necessary background to be able to effectively use curriculum that has been prepared by other organizations ~ if this curriculum is grounded in the research insight and uses effective risk prevention messaging.
- ✦ In evaluating curriculum for adoption, it is recommended that schools:
  - ‣ Request information on the research insight into youth risk online that has been relied upon in creating the curriculum. Check to see that this is based on academically valid research.
  - ‣ Ask the organization to describe the evidence-grounded risk prevention approaches that have relied on to create the curriculum.
  - ‣ Review the curriculum in the context of the research insight presented within this material.
  - ‣ Evaluate the curriculum to determine whether it uses any of the above problematical approaches.

To Protect Kids ~ Educate Parents

- ✦ To protect children, it is necessary to educate parents.
  - ✓ Educate parents about how to set up safe places for their child online. This can be accomplished with parent attention or the use of family safe features. (More on parent education below.)
  - ✓ Provide simple guidelines to children.

Tween and Teen Empowerment

- ✦ Starting in 4th grade, the focus should be on imparting the knowledge, skills, and values to engage in effective decision-making. The degree of sophistication in such decision-making will obviously strengthen as they grow.

Focus on Harmful Consequences

- ✦ There are risks associated with crossing a busy street. There are risks online. Students need to

understand the risks, know how to protect themselves, and respond to negative situations.

✓ Emphasize harmful consequences to themselves, as well as others, as a result of public and possibly permanent demonstration that they make bad choices.

- Use real examples to illustrate the potential harmful consequences of online actions. News stories will provide excellent "teachable moments" ~ as do incidents students experience, witness, or have heard about.

Common Standards

✓ Discuss the common values and standards.

- Terms of Use Agreements for sites.
- School's Internet use policy.
- Family's values.

✓ Ask them why there is so much similarity.

Information Credibility

✓ Address information credibility. Students must understand that anyone can post anything online ~ accurate or not~ and they must always read with their eyes open.

- Information credibility will be address extensively in the materials that will address Digital Media Literacy.

Effective Problem Solving

✓ Teach effective problem-solving skills. The teen years are when the brain's frontal lobe decision-making skills develop ~ give them practice in making good decisions.

✓ Use real world examples and ask them to evaluate what is happening and why.

- What is happening?
  - Who is involved?
  - What is or was each person trying to accomplish (have fun, get attention, get someone to stop doing something, get someone to do something, make friends, experiment, express a feeling)?
  - Is someone trying to manipulate someone else? How?
- What might happen to each person involved ? Would this be good or bad?
  - What harm or risks has someone caused or could come to others because of what this person has done?
  - What did any of the participants fail to think about?
- If you witnessed a situation like this what could you do that could help the most? If that didn't work, what else could you do?
  - If someone involved in this kind of situation was your good friend, what actions would you recommend to that person? If the person refused to listen to you, what other actions could you take?
- What are your personal standards and guidelines for your own online actions related to this kind of a situation?
  - What steps can you take to avoid getting into this kind of a situation? If you were in this situation what are the possible things you could do?
- If you had the same goal, how could reach it without hurting yourself or others?

Ethical Decision-Making

✓ Teach them to ask questions to make ethical choices.

- Is this kind and respectful to others?
- How would I feel if someone did the same thing to me, or to my best friend?
- What would my mom, dad, or other trusted adult think or do?
- Would this violate any agreements, rules, or laws?
- How would I feel if this was posted on the school bulletin board for everyone to see?
- What would happen if everybody did this?
- Would it be okay if I did this in Real Life?
- How would this reflect on me?

Online "Traps"

✓ Teach them why teens might make bad choices online and encourage them to watch for these traps:

- They think they are invisible and so won't be caught.
- They do not recognize that their online actions have harmed others or themselves ~ or the deception of others.
- They act fast ~ especially when angry ~ and forget that the material you post in electronic form can easily become very public and possibly permanent.
- They follow others who make bad choices.
- Think because they can it is okay
- They look for friends in the wrong places and find the wrong kinds of friends.

Youth Leadership

✓ Encourage them to be leaders.
- Model good choices online.
- Speak up for good values.
- Offer help or guidance to someone who is being harmed or making a bad choice.
- Report online concerns to a trusted adult and/or the site.

✦ Strategies to enhance youth leadership

✓ Stress the importance of helping others.

✓ Make sure they fully understand the potential harmful consequences on others.

✓ Provide practice in helping skills. “If you saw that a friend was … what would you do?”

✓ Ensure it is very easy for them to confidentially report concerns at school.

Parent Guidance

Guidance for Parents of Children

✦ To protect children we must educate parents. When children are young, it is a parent’s responsibility to make sure their Internet use is in a safe online environment and they engage in safe communications.
- Children who still believe in the tooth fairy cannot be expected to protect themselves online. To them, the Internet is more of a “magic box.”
- Even by 3rd grade and definitely by 4th grade, young people can begin to grasp essential concepts about how the Internet functions ~ which provides the ability for them to take on more personal responsibility for good decision-making.

✦ These are steps educators can advise parents to take:
- Remain actively and positively involved. Help your child learn to make good choices based on your family’s values.
- Create a “fenced play yard” for your child online. Limit your child’s access to sites you have selected as appropriate, unless you are present to closely supervise more expansive explorations. Jointly approve additions to this “play yard.”
  - Look into using the newer family safety features of your operating system, browser, or provided as a service by sites, and on interactive gaming consoles. These new family safety features allow parents to limit their child’s access to selected sites, control who has the ability to communicate privately, manage time spent online, and review the history file. Your child should know that everything he or she does online is open to your review.
- Keep the computer in a public place in your house so you can remain engaged in what your child is doing.
- Make sure you have implemented appropriate security against malware, use a spam blocker, block pop-up ads, and use safe search features. Never allow peer-to-peer software ~ a significant source of malware.
- Do not allow your child to register on sites for users over the age of 13. If your child’s friends are on these sites, talk with their parents. Find a safer place where the friends can communicate and share.
- Make sure you personally know everyone your child is able to communicate with through email and instant messaging. Limit communication with strangers to moderated children’s sites.
- Watch out for market profilers and advertisers. Commercial children’s sites provided for free are making money through advertising or are themselves an ongoing advertisement.
  - To allow for more effectively targeted advertising, some sites seek to determine your child’s age, gender, location, and interests. Some sites use surveys, quizzes, or contests to obtain more information. Read the privacy policy on sites carefully. Watch for “advergaming” ~ ads integrated into games ~ and sites that ask your child to sign up to receive ads or send ads to their friends. Sites by non-profit organizations and sites that charge a modest fee do not present these concerns.
  - Advertising to children is associated with consumption of junk foods, obesity, harm to self image, excessive consumption, and parent-child conflict. Make your selections carefully - based on your own degree of comfort with these practices.

- Help your child create a safe and fun username that does not disclose personal details and a safe password. Make sure your child knows to never disclose a password to anyone other than you. Use your email address for any site registrations.
- Never overreact if your child reports an online concern to you. You want your child to feel comfortable reporting online concerns - especially when your child becomes a teen.
- If your child engages in inappropriate or harmful behavior, impose a logical consequence that will focus your child's attention on the harmful consequences of his or her actions. Require that your child remedy any harm.

Savvy Parents of Tweens and Teens

✦ Encourage parents to be actively and positively involved:

- Appreciate your child's online activities. Show interest in your child's online friends. Work in partnership to address any concerns.
- Make sure you have implemented appropriate security against malware, use a spam blocker, block pop-up ads, and use safe search features. Never allow peer-to-peer software.
- Encourage your teen to always use the protective features on social networking sites and instant messaging to control who can view information and communicate in these personal environments.
- Keep computer in a public area until teen is older and has demonstrated good choices.
- Pay attention to what your child is doing online. But balance supervision with your child's legitimate interests in personal privacy. Positive interactions will encourage your child to share.
- Never overreact if your child reports an online concern. Fear of overreaction and loss of access is leading many teens not to report.
- If your child engages in inappropriate or harmful actions online or using a cell phone, impose a consequence that will focus attention on why those actions caused or could cause harmful consequences. Require a remedy for any harm.
- Pay attention to "red flags" ~ appearing emotionally upset during or after use, disturbed relationships, too much time online, excessively secretive behavior, and subtle comments about online concerns. Carefully try to engage your child in discussion.
- Encourage your child to help others directly or report to an adult if he or she witnesses someone being harmed or at risk online.
- Help your child learn to make good choices. Emphasize: "What you do online reflects on you."

School Staff Online

In Public Online

✦ School staff will always be "in public" online.

- Everything school staff does online ~ information and images posted, as well as friends ~ will be used to judge their character.
- Privacy protections will not prevent disclosure.
- Concern also relates to what friends of school staff might post that discloses unflattering information about the staff member ~ especially tagged pictures.
- All material will be used to ask one question: "Are you the kind of person we trust to be responsible for our children?"
- School employees can be disciplined for off-duty conduct if the school district can show that the conduct had an adverse impact on the school or the teacher's ability to teach.[10] Non-tenured teachers have even fewer protections.

Socializing With Students

✦ School staff should avoid socializing with students online, especially on social networking sites. "Socializing" means mixing socially - being friends. This does not include communications related to assignments or school activities. The concerns:

- Students flirt. If a student sends a flirtatious message to a staff member, that staff member

10 Simpson, M.D. (2009) *The Whole World (Wide Web) is Watching*. NEA http://www.nea.org/home/12784.htm

is in serious trouble. Respond warmly ~ accusation of sexual solicitation. Turn student down ~ face possibility of revenge.

- Students send friendship requests to friends of friends. Staff member would become "guarantor" of all friends.
- If a teacher "friends" some students, but not others this could create a perception that these students are favored and will receive a better grade.
- The risks: public censure, loss of job, loss of license, criminal prosecution, life as registered sex offender.

✦ Staff should be able to communicate with students related to classwork and school activities through a school-based Web 2.0 system and district email.
- These are school related communications where distinctions of status are maintained. These are not social communications

Staff Guidance

✦ Think before you post.
- Never post material that will raise questions about your character and values.
- Don't allow others to post such material about you.
- Always communicate as a professional ~ even if you are using protection features on social networking sites.
- Exercise extreme care when communicating online with students ~ avoid socializing.

✦ Districts should ensure there is a policy that addresses inappropriate relationships between staff and students.

Part II ~ Internet Safety Education

Introduction

Student Guides have been provided by CSRIU for different grade levels: K-1, 2-3, 4-5, 6-8, and 9-12.

These grade guides should be assessed based on insight about the online activities of the students in your local community. The age at which these young people are becoming engaged online and these issues come up seems to be reducing steadily and there appears to be some regional differences Therefore, it may be appropriate to use the 2-3 materials in 1st grade, the 4-5 materials in grade 3, the 6-8 materials in 5th grade (consider this after sex education instruction), and the 9-12 materials in 7th and 8th grades. Remember, 11 year olds are joining social networking sites and sending nude images to peers.

CSRIU materials are in the form of messaging ~ not specific curriculum. It is the perspective of CSRIU that by the time students are in middle school, material that is perceived to be "professionally developed curriculum" may not be as accepted by students because it has an "authoritarian feel."

It is recommended that teachers establish an environment where students discuss these issues starting with a focus on news stories or incidents they have witnessed or experienced. Strive through the use of guided questions to assist the students in developing similar standards in their own "voice." Teachers may provide the CSRIU materials to the students or use them for their own reference to guide the questions they ask students. Several lesson plans are set forth in the Appendix.

Cyber Safe Kids

Primary Grade Messages (also Pre-K)

Simple Guidelines

✓ Provide simple guidelines for primary grade students.
- For younger students, staying on the safe sites, not typing their name or other contact information, and knowing how to turn off the monitor if something "yucky" emerges.
- The time to expand to the additional guidelines ~ found in the grade 2-3 materials is when they are able to start communicating

in written form. For many students, this will be first grade.

Instructional Objectives

- (K-3) Students will recognize that there are many web sites that have material that is not designed for children and will collaborate with their parents in remaining on the sites that are safe, fun, and appropriate.
- (2-3) Students will recognize that time spent using electronic devices should be kept in balance with other activities.
- (2-3) Students will recognize that material posted in electronic form can be provided to others and that others will judge them based on what they have posted.
- (K-1) Students will recognize that they should not type their name, address, or phone number online. (2-3) Students will describe important actions to protect their personal information online, including not typing their name, address, phone number, sending a picture, or completing an online form without checking with a parent and not providing their password to anyone other than a parent.
- (2-3) Students will distinguish between personal communications including email and instant messaging, and public sites such as fun game sites and will know that they should only communicate with friends through personal communications.
- (2-3) Students will recognize that people can be mean online, describe the steps they should take if they receive a nasty message on a public site or through private messaging, and describe personal standards for how they will treat others online.
- (K-3) Students will recognize that sometimes, through no fault of their own, "yucky" material could appear and that if this happens they should immediately turn off the screen and tell an adult and will demonstrate the ability to rapidly turn off any computer they use while at school.
- (2-3) Students will explain that the purpose of advertising is to try to convince them to request that their parents purchase something for them, and demonstrate the ability to distinguish between advertising and content on web sites.

Key Safety Rules for Primary Grades

Have Fun Online in Safe Places

- Use the fun sites that you and your parents have selected. If you want to go to a new site, ask permission.

Keep Your Life in Balance

- Have fun online. But make sure you do other fun things and get together with your friends to play.

Keep it Secure

- Use a safe password ~ with letters and numbers. Never share your password with a friend.
- If your computer starts acting "weird" ~ tell your parent.

Think Before You Post

- Be the best you can be online. Remember anything you post or send online can be sent to others.
- Never type your name, address, or phone number online, send a picture, or complete an online form without first checking with your parent.

Connect Safely

- Communicate only with friends through email or instant messages. Communicate with strangers only on safe kid's sites.
- If someone sends you a mean or nasty message on a public site ~ don't respond. Ask your parent for help to file a complaint on the site.
- If a friend sends you a mean or nasty message ~ calmly and strongly tell your friend to stop. Ask your parent for help.
- Never send mean or nasty messages.

Turn It Off & Tell

- If anything yucky ever appears when you are online ~ quickly turn off the screen and tell an adult.

Spot the Ads

- Many web sites have ads for things kids like to buy. See if you can spot the ads. Some sites have banner ads. Some sites are ads for toys. Some sites have games you can play that are really ads..
- Remember, you do not need to buy everything you see in ads.

Cyber Savvy Kids ~ Tweens ~ Teens

Intermediate, Middle School, and High School Messages

Although these grade ranges are grouped, there is obviously a significant developmental range. The reason these are grouped is student's ability to engage in independent problem-solving starts to kick in after they move beyond the "magic years." The objectives set forth increasingly sophisticated problem-solving strategies.

The second major "shift" in development comes around age 12, when the "raging hormones" kick into full gear. By the age of 13, young people are able to enter all general audience sites. But many are lying about their age and entering these sites at a younger age. It is advisable that the guidelines for students in grades 9-12 be introduced in 7th grade.

The primary difference between the 6-8 and 9-12 materials is the manner in which social networking and risky sexual relationship issues are addressed. In some communities it is not considered appropriate to discuss sexually-related issues with middle school students. Further, students are not supposed to be registering on social networking sites until they are 13.

Foundational Protections

What You Do Reflects on You

Make Good Choices Online

- The discussion on negative influences on online behavior and effective decision-making was in the previous sections.

Instructional Objectives

- (4-12) Students will recognize that their online actions, which are recorded in electronic form that can be widely disseminated, can affect their reputation, friendships, and opportunities.
- (4-12) Students will determine the appropriateness of online actions using self-reflection questions that will seek to address the potential negative influences on behavior and lead to safe, ethical, and responsible choices.
- (4-12) Students will recognize the key negative influences on online behavior, including the perception of invisibility, lack of tangible feedback, acting without thinking which may result in posting damaging material in electronic form, being negatively influenced by others, and thinking that because they can easily do something using technology this gives permission, and describe strategies to avoid online actions that have been negatively influenced.
- (4-12) Students will identify actions they can take to demonstrate online leadership particularly if they witness a situation online that could lead to a harmful consequence to another, including speaking out for good values online, helping someone who is at risk or being harmed, and reporting significant concerns to an adult.
- (6-12) Students will apply questions they can ask themselves to engage in effective problem-solving to develop appropriate actions(s) in response to potentially harmful online situations, including an analysis of the situation, identification of potential harmful consequences, developing possible actions, and evaluating possible outcomes to those actions.

Keep Your Life in Balance

Avoid Addictive Access

- The research in this area is somewhat mixed.
  - Some research appears to indicate that teens who are highly social ~ involved in many school activities ~ are simply also highly active online.[11]
  - But Internet addictive access is being considered for inclusion in the Diagnostic and Statistical Manual of Mental Disorders - V as a compulsive-impulsive spectrum disorder.[12] At least three subtypes: Excessive gaming. Sexual preoccupations. Email/text messaging.
- The APA has identified four components of harmful addictive access:

11Lenhart, A., Madden, M., Rankin, A., & Smith, A., (2007) *Teens and Social Media: The use of social media gains a greater foothold in teen life as email continues to lose its luster*. Pew Internet & American Life Project. http://www.pewinternet.org/PPF/r/230/report_display.asp.

12 Block, J.J. Issues for DSM-V: Internet Addiction, *The American Journal of Psychiatry*. http://ajp.psychiatryonline.org/cgi/content/full/165/3/306.

- Excessive use, often associated with a loss of sense of time or a neglect of basic drives.
- Withdrawal, including feelings of anger, tension, and/or depression when the computer is inaccessible.
- Tolerance, including the need for better computer equipment, more software, or more hours of use.
- Negative repercussions, including arguments, lying, poor achievement, social isolation, and fatigue.

Instructional Objectives

- (4-12) Students will identify indicators that can determine whether the amount of time they spend using electronic devices is interfering with other important activities. Indicators include:Spending more time more time online than planned. Use Internet late into the night. Fatigue. Spend time online instead of other activities. Preoccupied with online activities. Depression or anxiety. Argue about time limits.
- (4-12) Students will describe strategies they can use to keep their time using electronic devices in balance with other important life activities, including setting goals and keeping track of time, making plans for other activities, avoiding being online when doing homework, and turning cell phone off at night.

Think Before You Post

Protect Your Personal Information & Reputation

- Some young people appear to be unaware that postings are public and possibly permanent, material shared privately can become public, and this can place them at risk or damage their relationships and future opportunities.
- The Internet Law of Predictable Consequences.
  - The more embarrassing, outrageous, or damaging the material you post or send privately ~ the more likely it will become very public and be seen by people who will judge you badly. If you would not post it on a bulletin board at school ~ don't post or send it!
- Too often, Internet safety messages warn against posting personal contact information ~ name, address, school, sports team ~ presenting the fear that if they post such information some online predator will track them down and abduct them.
  - There is no evidence that this is happening![13] The risk of sexual exploitation associated with posting information is posting sexually provocative images. So let's tell them that. If guidance on posting personal information is tied to fear of predators, students may dismiss the guidance.
- What students need to know is that there are different kinds of information about themselves or others that could be posted, different places where they might share this information, and different recipients who might receive or be able to access the information.
  - The risks are associated with the kind of information shared and to whom.
- Under the Children's Online Privacy Protection Act, web sites must limit the information they can request from children under the age of 13.[14] COPPA restricts the kind of information children can post on the sites.
  - By age 13, young people are generally considered to be functioning like adults on general audience sites (not adult sites). By this age, there are no restrictions on the information that can be requested.
  - But many young people are lying about their age to register on these sites, especially in middle school. So they need to know how to address these issues ~ preferably without the adult appearing to condone such registration.
- Young people are posting material that appears to be either threatening or distressing ~ that could indicate they are contemplating an act of violence against self or others.[15]
  - But students are also incapable of fully understanding how material they post as a "joke" might be misinterpreted and could lead to significant problems for them.
  - Threatening or distressing material is far more likely to be witnessed by other teens, therefore encouraging students to report is critically important.
- The online sites that most teen (and tweens) post information is on social networking sites. One of the most important steps in protecting personal

13 http://www.unh.edu/ccrc/internet-crimes/safety_ed.html.

14 http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

15 CSRIU has a full presentation for safe school personnel addressing this issue.

information is using the protection features on these sites.

- It is very important to emphasize that "protected" does not mean "private" - not if they have more than one friend.

✦ Teachers will note a difference in approach on these issues between middle and high school. The reason for this difference is the perspective that high school students will be taking on more personal responsibility for information-sharing.

Instructional Objectives

✦ (4-12) Students will recognize that any material they post or send in electronic format can easily become very public, potentially permanently available, and damage their reputation and interfere with current or future opportunities.

✦ (4-12) Students will distinguish different kinds of personal information about themselves or others, recognize the risks associated with disclosure of such information, identify different kinds of online environments where such information might be disclosed, identify possible recipients of such information, and demonstrate effective strategies to protect against disclosure of personal information in a manner that could cause harm to reputation or opportunities.

- (4-12) Personal interest information includes interests and activities. This is generally safe to share on protected profiles or on safe online community sites. Such information could be used to direct advertising to them.
- (4-8) Personal contact, financial, or identity information includes full name, address, phone numbers, email/IM address, passwords ~ and any identification or debit/credit card numbers. This could make it easier for an unsafe person to find them, be used to send them advertising, obtain access to their accounts, or for identity theft. This information should not be shared without parent permission.
- (9-12) Personal contact information includes name, address, phone number, and email/IM address. Disclosure could lead to unsafe contact or advertising. Other than their name, should generally not be posted online. This information should never be shared with an online stranger. Avoid providing on web forms, unless for a legitimate purpose, like a purchase.
- (9-12) Financial identity includes any personal identification or financial account information, including passwords. This can be used for identity theft. Should only be shared with parent permission on secure web sites. Never share passwords.
- (4-8) Unsafe personal information is information that makes them appear vulnerable, unkind, or that they make bad choices, or any information they want to be kept secret. This could could be used to manipulate them or disseminated to harm their reputation. This information should never be posted or shared publicly or privately.
- (9-12) Intimate information is sensitive personal information that makes them appear vulnerable or they want kept secret. This could be used for manipulation or disseminated to harm their reputation. Should never be shared in public. Best not to share even with a friend in private. Share with care on a professional support site.
- (9-12) Reputation damaging material can ruin reputation, interfere with opportunities, and damage personal relationships. Never share publicly or privately.
- (4-12) Damaging information about others could harm them. Never share publicly or privately.
- (4-8) Damaging information about them posted by others could harm their reputation and opportunities. Tell an adult. File a complaint with the site.
- (9-12) Damaging information about them posted by others could harm their reputation and opportunities. Demand it be removed. If it is serious or not removed, tell an adult. File a complaint with the site.
- (4-12) Threats could be real or not. Never post material that someone might think is a threat. Always report a possible threatening situation because if it is real, someone could get hurt.

Connect Safely With Others

Interact Safely With Others Online

✦ Young people can be expected to interact with friends, acquaintances, friends of friends, and strangers. Any can be safe ~ or present risk.

- The research demonstrates that online interactions with known peers are causing the most emotional distress.[16]

16 See Berkman report, footnote 2.

- Anyone who the young person does not know very well in Real Life requires special consideration because they can present greater risks because this person could be deceptive and it is more difficult to perceive the deception.
- People who no one they know knows in person present the greatest risk. Sometimes this could actually be someone they do know who has created a fake profile. Deception is also exceptionally difficult to detect.

✦ It is important to distinguish between public communication environments and personal communications.

- Public environments are places where many people engage in communications. This includes gaming sites, discussion forums, chat rooms, and the like.
  - Safety depends on kind of site. Children's sites that attract other children and have good rules and moderation are generally safe. Environments that attract teens and adults present greater risks, especially depending on subject of communications.
- Private communications include email, instant messaging, and social networking messaging that are protected.
  - All of these environments have protective features that allow users to restrict who can communicate. Use of such features should be strongly encouraged.

✦ Most of the time, young people will communicate with safe strangers on gaming sites or friends, acquaintances, or friends of friends on social networking sites. But they could run into "nasty online people." Here is the list of "nasties:"

- Posers. People who post material about themselves that is not true. Many times teens will share information that is not totally accurate. The concern comes if they are thinking of taking an action, **especially** one that could harm them, based on what someone has told them online. Guidance is to take time to get to know people online. Carefully review postings ~ knowing the information shared could be false. Watch out for inconsistencies. Trust their "gut."
- Impersonators. People who break into someone's account or create a profile that appears to be someone ~ for the purpose of sending messages or posting material that will damage the reputation of that person. Always protect their password. If someone has impersonated them ~ secure their profile or file a complaint. Tell a parent.
- Fakes. False profiles that have been set up to trick and humiliate someone. If neither the young person nor any of his or her trustworthy friends knows that "hot" teen who wants to "friend", this could be a fake profile set up to hurt the young person. Don't "friend" strangers on a profile or in instant messaging. Exercise care in any public group.
- Griefers. People who join games or other groups for the sole purpose of interfering with the enjoyment of others ~ to cause grief. If someone responds with anger or a counter attack, this is just what the griefer wants. Ignore or block the griefer or file a complaint.
- Creeps. People who try to manipulate young people into doing something ~ that will likely end up hurting or humiliating them. Creeps often send overly friendly messages, tell the young person how "hot" he or she is, offer gifts or opportunities, try to push them into a special secret relationship, ask for a sexy picture, and try to turn them against their parents or friends. Don't let creeps manipulate. Show any messages from a creep to an adult. Creeps can be dangerous.
- Downers. People or groups that encourage harmful things like anorexia, self-cutting, hate, or gang activity.[17] These kinds of people or groups do provide emotional support ~ but at a very harmful price. They will take young people "down." They may require that a young person prove he or she "fits in." They argue that these activities are okay ~ but the actions they encourage will cause harm or could harm others. Don't let any person or group lead them in a direction that is not healthy and happy.

✦ Sometimes teens will want to meet in person with someone they have gotten to know online. In the vast majority of these situations, this is just a meeting with another teen, generally a friend of a friend. But these situations could present risk.

- If we just tell them "no," many may meet anyway and may not take steps to be safe. They need to know how to meet safely. This includes meeting in a public place, with friends or parent present, a well-thought-out "escape"

17 This issue is addressed more comprehensively in CSRIU's Youth Risk Online presentation and below, under Specific Risks..

plan, and parent approval (and approval of friend's parents).
  - Especially in high school, they are unlikely to take a parent to such meeting, but will willingly bring a friend.

Instructional Objectives

- (4-12) Students will describe basic safety practices including username selection, use of protective features, and how to safe harmful messages, block unwanted people, and file a complaint in every communication environment.
- (4-5) Students will recognize the dangers presented when interacting with someone online who is not known in person. communicate with friends only in personal communications, and strangers only on fun kid's sites.
- (4-5) students will recognize the need to discontinue communications with anyone who is overly friendly, weird, or hurtful.
- (6-12) Students will recognize the dangers presented when interacting with someone online who is not known well in person, including acquaintances, friends-of-friends, and strangers. Students will explain safe practices for safely interacting with these people.
- (6-12) Students will recognize the importance of exercising care when getting to know people online and recognize the risks presented by others who are presenting false information, my try to impersonate them, have created a fake profile, are causing grief, may be trying to manipulate them, or may be trying to encourage involvement in unsafe actions.
- ((4-12) Students will recognize the potential risks of meeting in person with someone who they have gotten to know online and describe steps to take to arrange for a safe meeting, including meeting in a public place with parent or friends present, a well-designed escape plan, and parental approval.

Sites & Security

Keep Yourself Secure

Implement Security & Avoid Scams

- Parents should have the responsibility to ensure the security of home computers. But given young people's advanced technical skills and behavior that could lead to security concerns, it makes sense to involve them.[18]
- Essential protections include:
  - Install firewalls and computer security software.
  - Create safe password with letters and numbers.
  - Use a spam blocker.
  - Configure browser to block pop-up ads.
  - Do not install peer-to-peer networking software.
  - Set search engine preferences to filter results.
  - Only download from safe sites.
  - Don't open unsolicited or unknown email messages or open attachments from people they don't know or don't expect.
  - Never reply to or click on links in email or pop-ups that ask for personal information.
  - Recognize that if their computer starts acting slow or accesses sites that they don't want to access, tell your parent. This is a sign your computer has been infected.
- Many scams seek the disclosure of financial identity information, which has already been addressed, or efforts to trick the person into doing something that will allow an invasion of their computer security, generally also for the purpose of identity theft. Scams tend to have two identifying characteristics:
  - Offers that are "too good to be true" or offer something really cool for no or little risk.
  - Threats that something bad will happen if they do not disclose personal information.

Instructional Objectives

- (4-5) Students will describe the actions necessary to ensure effective computer security and will ask parent approval before registering on sites.
- (6-12) Students will describe the actions necessary to ensure effective computer security.
- (6-12) Students will recognize indicators of a scam, including offers that are too good to be true and threats that if they do not disclose personal information something bad will happen to their account.

18 The Federal Trade Commission's OnGuard Online web site contains very helpful guidance on both of these topics. This material is very helpful for instruction. http://www.onguardonline.gov.

Abide by the Terms

Follow the Terms of Use

- In schools, students are required to abide by the terms of the Acceptable Use Agreement (AUPs). When they become employees, there will be workplace AUPS. Interactive web sites, where users are allowed to post material, have Terms of Use Agreements.
- All AUPs and Terms of Use Agreements contain provisions for behavior that is deemed unacceptable because the behavior could harm others or the integrity of the system or site.
  - Both in school and in the workplace it is important that users restrict their use to education or employment purposes.
- One instructional activity for this issue is to ask the students to bring in a copy of the terms of use agreements of their favorite web sites and provide the district's Internet use agreement. For 9-12 grade students also obtain some of the employee terms of use agreements from local employers and government agencies.
  - Have the students compare and contract the provisions ~ especially noting the similarities.

Instructional Objectives

- (4-12) Students will describe the common provisions of school and employee acceptable use agreements and terms of use agreements for social networking sites and explain the purpose for such provisions are to prevent harmful consequences to others or the site and will recognize that the consequences for violating such terms generally involve restrictions on use or other discipline.
- (4-12) Students will distinguish the difference between online socializing and the use of technology resources for educational and (6-12) for employment purposes.
- (4-12) Students will demonstrate the ability to guide their online activities while at school in accord with provisions of the district's Internet AUP including the educational use restriction.

Stay Out of the Garbage

Avoid "Gross Stuff"

In a 2005 survey, the authors found that 13% of youth Internet users 10 through 17 years of age visited X-rated Web sites on purpose in the past year. However, even more youth (34%) were exposed to online pornography they did not want to see, primarily through (in order of frequency) links to pornography sites that came up in response to searches or misspelled Web addresses or through links within Web. sites, pop-up advertisements, and spam e-mail.[19]

- False security. The over-reliance on filtering has resulted in a failure to teach students how to avoid accidental access and respond.
  - Filters will never be entirely effective ~ especially in blocking newer sites or "porn traps."
  - Efforts to provide technical strategies for dissidents in countries in the Middle East and Asia has resulted in the ability for any technically sophisticated teen to easily bypass filtering software. Conduct a search on "bypass Internet filter."
- Accidental access can be reduced by effective technical prevention and safe searching strategies.
  - The possible emotional harm can be reduced by making sure every student knows exactly what to do if something bad comes on the screen.
- Most teens, especially teen boys, will spend sometime looking. The concerns are the amount of time and the kinds of material. This may be an issue to address in a sex education discussion - but will likely be controversial. For the purposes of Internet safety, students can be warned that such material often comes with malware that can mess up their computer.
- Technical prevention: Effective computer security. Filtered search returns. No peer-to-peer networking software.
- Safe surfing strategies:
  - Read, think, then click. Don't click on suspicious links.
  - Don't fall for traps. Don't type a URL ~ type the name of the site in a search engine.
  - Can the porn spam. Don't open suspicious email messages or click on their links.
- Appropriate responses.
  - Turn it off and tell. Turn off the monitor, force-quit the browser, or turn off the computer. Tell an adult what happened ~ so you won't be blamed.

---

19 Wolak, J., Mitchell, K. J., and Finkelhor, D. (2007). Unwanted and wanted exposure to online pornography in a national sample of youth Internet users. *Pediatrics*, 119(2), 247-257. http://www.unh.edu/ccrc/pdf/CV153.pdf.

- Make sure someone evaluates the computer to take any necessary corrective actions.

Instructional Objectives

- (4-12) Students will describe the techniques they can use to avoid accidentally accessing objectionable material and the actions they should take if such accidental access has occurred.
- (6-12) Students will understand that often objectionable material comes with malware.

Don't Sell Yourself

Watch Out For Aggressive Profilers and Advertisers

- Track ~ Trick ~ Target. Children and teens are "hot prospects." Advertisers can track, trick, and target them largely outside of parent awareness. Children and teens do not understand these issues. Most of the sites that are attractive to children and teens are supported through advertising. This means most sites are engaging in:
  - Market profiling ~ creating database of contact information, interests, activities, and friends
  - Targeted advertising ~ using profile to target advertisements. This is also called "behavioral advertising."
- A frequent statement of marketers is that people want them to know what they are interested in so they can receive ads that would be of interest. An exceptionally important study, entitled *Contrary to what Marketers say, Americans Reject Tailored Advertising and the Three Activities That Enable It*, found:[20]

  > Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%--say they would not want such advertising.

  - This report did NOT ask the respondents what they thought about web sites engaging in engaging in behavioral advertising directed at children and teens. But this is what is happening.
- The U.S. Federal Trade Commission is striving to address this issue.[21] Industry is responding by indicating they are providing greater transparency and user control.
  - This will not work unless users become better educated. And the vast majority of adult users have no idea how behavioral advertising actually works.
  - It is the author's opinion that greater restrictions should be placed on profiling of children and teens because young people absolutely do not have the cognitive development to be able to effectively understand these issues and the ramifications.
- As noted before, the Children's Online Privacy Protection Act was supposed to act to limit this. Limit information collection of children under 13.
  - COPPA requires privacy policies. But many parents do not understand profiling and most privacy policies make it sound like the site protects privacy.
- Here is an example of what a "privacy" policy for a teen site might say.[22]
  - This site collects user information on certain portions of our site, through methods which include, but are not limited to, responding to questions and surveys, registering for the site, or through various offers provided on site. By submitting personal information you grant site the right to use that information for marketing purposes including, but not limited to, sharing such information with advertisers. This site may also use such information to deliver certain direct marketing offers to you via telemarketing, e-mail marketing, direct mail, SMS messaging and other types of direct marketing. We may sell the personal information that you supply to us to selected third parties, including direct marketing services. By agreeing to these terms, you hereby consent to disclosure of any record or communication to any third party when The site, in its sole discretion, determines the disclosure to be appropriate.

20Turow, J., King, J., Hoofnagle, C.J., Bleakley, A. and Hennessy, M., (September 29, 2009). http://repository.upenn.edu/asc_papers/137/.

21 http://www.ftc.gov/opa/2009/02/behavad.shtm

22 This language came from the Quiz Rocket site at http://www.quizrocket.com - a popular personality quiz site. Their new policy provides less insight into what information the site collects and how it is used, and also an obfuscatory provision that ostensibly offers an "opt out." The reason this policy language is included in these materials is that it so well describes what ,most sites are actually doing.

- Online advertising. The following are common online advertising techniques:
  - Banner ads ~ targeted to interests.
  - Advergaming ~ integrating ads into games or attractive fun profiles on social networking sites.
  - Permission marketing ~ asking users to sign up to receive ads.
  - Buzz or viral marketing ~ asking users to send ads to your friends.
- Harms of advertising. Research has shown that advertising to children and teens leads to unhealthy values, consumption, and behavior: [23] Obesity and poor nutrition. Parent-child conflict. Encouragement of violence. Sexualization and harmful self-image.
- An instructional approach to address these issues is
  - Ask the students to do a web quest.
    - Find and evaluate a privacy policy, especially on a social networking and personality quiz site.
    - Find a banner on your profile that appears to be targeted based on specific information the site knows about you.
    - Find examples of an advergames and buzz marketing.
  - The students could create a slides presentation or poster setting forth what they found.
  - HIgh school students could read the above-mentioned report and materials on the FTC web site. Ask them to develop personal standards or encouraged them to draft a joint letter to your local members of Congress describing what actions they think should be taken to address market profiling of teens and children.

Instructional Objectives

- (4-12) Students will recognize that most of the sites they visit are supported through advertising revenues and that this often leads to efforts to create a market profile of their demographics and interests that will be used to direct specific advertisements to them.
- (4-12) Students will describe the various forms of advertising online, including banner ads, advergaming, permission marketing, and viral marketing.
- (4-5) Students will know to ask a parent before providing personal contact information or responding to a quiz or game that asks them about personal interests.
- (6-12) Students will identify the specific techniques used online to obtain their demographic and interest data and recognize that much of what they post online will be reviewed for the purpose of advertising.
- (6-12) Students will develop personal standards regarding the amount and kinds of personal information they will provide when such information is specifically solicited or when they have the opportunity to control such the collection of such information.

Protect Your Face & Friends

Protect Your Reputation & Circle of Friends When Social Networking

- Social networking sites allow teens to create personal profiles, post images and writings, connect with friends.
  - The risks include: Posting material that ruins their reputation or that others could use against them. Connecting with unsafe people. Being hurtful to others ~ or having others be hurtful to them.
- Most sites have protection features that allow users to set the profile to “private,” pre-approve comments posted by others, block unwanted contacts, and file abuse reports.
  - Protective features + reasonable care = safer place. No one can see a protected profile or communicate without a friendship link.
- At this point in time, all of the popular social networking sites restrict users to over 13 years old. But by middle school, many students are registering on these sites, generally with parent approval. This presents a difficult instructional situation because it is important to address the safety issues without appearing to condone the use of these sites by students who are not yet 13. Social networking sites for children appear to be emerging. Unfortunately, these do not appear to be very popular.

  Note: One difference between the 6-8 and 9-12 materials for students is that in the 9-12 materials social networking is addressed as a separate issue. This section essentially repeats guidance provided related to protecting information and interacting with

23 American Psychological Association, http://www.apa.org/releases/childrenads.pdf. American Academy of Pediatrics, http://pediatrics.aappublications.org/cgi/content/full/118/6/2563.

others. In the 6-8 materials, guidance on social networking safety is included in these other two sections. If the 9-12 materials are used in middle school, a possible message is: "We are going to discuss these issues so you are prepared to use these sites safely when you are enough and your parents have approved."

- ✦ The foundation for protection on these sites is:
  - ‣ Use protective features to limit who has access to information and can communicate.
  - ‣ Remember that "protected" does not mean "private" and therefore they should never post material that could damage their reputation, be used against them, or that causes harm to others.
  - ‣ Understand that their friends may establish links with the people they "friend." Therefore, they must protect their circle of friends by not friending an unsafe or unknown person.

Instructional Objectives

- ✦ (4-5) Not addressed.
- ✦ (6-8) Protection concepts, including using protective features, protecting personal information, and safely interacting with others, are addressed in other sections.
- ✦ (9-12) Students will describe the ways that social networking is allowing them to creatively demonstrate their personal identity and maintain connections with friends and identify the risks that may be associated with this activity.
- ✦ (9-12) Students will identify the protective features that are provided on the popular sites, explain how these features give them control over who can access their information or send messages, and develop personal standards to guide their use of these features.
- ✦ (9-12) Students will describe how what they post on their profile is used by others to form an impression of them and how this impression can impact their reputation, personal relationships, and current and future opportunities and develop personal standards regarding what they will post.
- ✦ (9-12) Students will explain how the process of "friending" leads to increasing circles of friends including people who they know as well as people who their friends know, but that establishing a friendship link to an unknown or unsafe person could potentially result in harm to a friend and develop personal standards for establishing a quality circle of friends.
- ✦ (9-12) Students will develop personal standards for use of protective features, the kinds of information and images they will post on personal profiles, and the connections they establish with others in social networking environments.

Specific Risks

Unsafe Online Communities

- ✦ The concept of "downers" is addressed in Connect Safely. This is introductory information related to a specific risk related to unsafe online communities or groups.[24]
  - ‣ Self-harm groups encourage such activities as self-cutting, anorexia, steroid or drug use, passing out games, and the like.
  - ‣ Dangerous groups foster hatred or harm directed at others, including hate groups, gangs, hacker groups, and the like.
  - ‣ These groups function with significant similarity in methods. They provide emotional support for "at risk" youth. They frequently have associated symbols, they may require "proof" that the members adhere to the norms of the group and ostracize anyone who is perceived to be "fake," and they rationalize their norms.
  - ‣ Research on this concern is just emerging. These groups will only attract a minority of youth, whose concerns probably are best addressed in the context of counseling. At this point in time, it is unclear how to address this concern instructionally. It is for this reason that there is not a separate section on this issue. The concept of "downers" can provide the opportunity for discussion. Especially encourage witnesses to report. When more insight is available, instruction will be provided.

24 This concern is addressed in greater detail in CSRIU's materials on Youth Risk Online.

Effectively Handle Mean Teens Online ~ Don't Be One

Prevent Cyberbullying[25]

- Cyberbullying is the use of electronic communication technologies to intentionally engage in repeated or widely disseminated acts of cruelty towards another that results in emotional harm.
  - New kind of "playground." Electronic aggression can range from minor incidents to devastating harm. Can happen 24/7 and be very public. Can lead to emotional distress, school failure, violence, suicide.
- Types of incidents: Flaming ~ online fights. Harassment ~ direct harmful messages. Denigration ~ indirect harmful postings. Exclusion ~ cutting someone out of a group. Impersonation ~ pretending to be someone to cause that person harm. Outing ~ posting privately provided damaging material. Trickery ~ fake profile or other tricks to cause harm. Cyberstalking ~ repeat online actions that cause fear.
- Schools must respond. Most cyberbullying is a continuation of ~ or retaliation for ~ on-campus bullying. It is negatively impacting school climate and leading to a hostile environment or violence at school.
  - Comprehensive bullying prevention is necessary. Involve safe school and educational technology. Focus on prevention and effective intervention ~ not simply discipline.
- Schools can respond. School officials have the authority to formally respond to off-campus speech that has ~ or reasonably could ~ cause a substantial disruption or interference with rights of students at school. But not merely displeasure of highly objectionable speech.

Building Teen Capacity for Prevention & Response

- The research has indicated that teens frequently do not report online incidents to adults either because they have already taken care of the situation ~ or they think they should be able to take care of these situations.
  - This is developmentally appropriate - they need to be able to resolve the vast majority of personal altercation situations by themselves. When they report to an adult, they frequently "lose face" with their peers and this can lead to greater problems. They will not tell adults, simply because we tell them to tell adults.
  - The CSRIU materials honor teen's desire to be self-sufficient by telling them how they can respond independently. These independent steps will likely be effective in resolving most situations. By honoring their desire to be self-sufficient, it is hoped that they will be more likely to request help when they really should.
  - The materials also advise them how adults can help ~ including providing "invisible assistance" so that their peers do not know they are getting help from an adult. It is important to mention that even adults sometimes have to get help from someone with greater power to resolve some problems ~ like human resources, attorneys, the police.

Prevention

- There is a social "pecking order" in schools where some stronger students pick on students identified as weaker or different. We must help students not be "weak birds" by doing something online that provides "ammunition" for others.
  - Warn against posting material others can use against them, accidentally offending others by not being careful how they communicate, or hanging around places where they are being treated badly.

Responding

- The most important step in an effective response is not acting when angry. The Latin quote that appeared in a Greek play Medea, by Euripides, "Whom the gods would destroy, they first make mad," may be a helpful concept to introduce. If they act when they are emotionally upset, they will likely not be as effective as they could be if they wait to calm down and consider their options.
- The corollary to this is not retaliating. Demonstrating that the bully has effectively gotten you angry only rewards the bully ~ and could make others think they are equally at fault.
- Saving the evidence and figuring out who the bully is are important steps.
- Then, the young person must figure out how to respond. As noted, the objective in these materials is to foster self resilience and effective responses ~ especially for the minor incidents that they can and should be able to resolve..

25 CSRIU has extensive materials available for safe school personnel to address this concern. This section will provide an overview.

- The other objective is to make it easier for teens to report these incidents to adults. This is done in three ways:
  - Communicating trust that they will be able to handle many of these situations on their own.
  - Reframing that asking an adult for help is not a sign of weakness, but a sign that they will not put up with being harmed.
  - Indicating that one way adults can help is by providing "invisible assistance" so that the student can, and is perceived as, responding on his or her own.

Not Being a Cyberbully

- The materials in this section are guided by insight into what motivates bullying. Key concepts include:
  - People do not "deserve" to be treated badly.
  - Bullying is not "cool" and will lead other people not to want to be friends.
  - Don't become a cyberbullying to retaliate against someone who is bullying them.
  - If they made a mistake and offended someone, apologize.
- Adult responses include providing invisible assistance, contacting the parents of the cyberbullying, or getting the school involved.
  - They also need to know that particularly egregious cyberbullying can lead to legal trouble. Law suits are being filed against parents of teens who are harming others. And some incidents are leading to criminal prosecution. These situations are best demonstrated using news stories.

Positive Peers

- Encouraging teens to provide leadership in stopping these incidents is very important. Strategies to encourage positive peer intervention were addressed above.
  - Instructionally, when discussing these issues with students, especially when discussing actual situations, it is advisable to ask how they would respond to a particular situation if they were a witness.

Stopping Flame Wars - and Reporting

- Flame wars are online fights that start small and build, frequently getting angrier and angrier and involving more and more students.
  - All students have important responsibilities in stopping flame wars. Those involved in an incident that appears to be growing need to simply back off. Those who are witnesses might be able to step in and stop the fight.
  - Students must know the importance of reporting flame wars involving students in a particular school to school officials, because frequently these flame wars lead to violence at school.

Instructional Objectives

- (4-12) Students will recognize how their online postings or communications might place them at risk and develop personal standards so that what they post cannot be used to cause harm to them.
- (4-12) Students will explain how a cycle of aggression that involves aggressive acts that lead to retaliation and increased aggression can grow to a point where all parties are being harmed, and describe strategies that can be used to effectively stop the expansion of such aggression.
- (4-12) Students will describe effective independent strategies to follow if someone engages in online aggression that targets them, including: Taking the time to calm down and consider possible actions. Not engaging in retaliation. Saving the evidence and identify the aggressor. Steps they can take to independently resolve the problem including leaving the site or ignoring the person, calmly and strongly telling the person to stop, blocking the person from communicating, or filing a complaint with the site or service.
- (4-12) Students will describe ways in which adults can help stop online aggression including: Providing "invisible guidance" to help them deal with the cyberbully. Contacting the cyberbully's parents. Obtaining assistance from the school. Contacting an attorney or the police.
- (4-12) Students will recognize: That the majority of their peers do not approve of aggression and think badly of people who engage in aggression. That retaliating online to someone who is bullying them will not resolve the problem and could lead to their being blamed for the problem
- (4-12) Students will develop personal standards to avoid engaging in online aggression.
- (4-12) Students will recognize that as witnesses to aggression they can play an exceptionally important role in preventing the continuation of the harm by helping the person who is being harmed, filing a complaint, negotiating a resolution, publicly or privately telling the aggressor to stop, or showing a trusted adult.

Cyberdate Safely ~ Avoid the Hurt

Avoid Risky Relationships & Activities

Note: Different communities will have different perceptions on what age is best to introduce these topics. The Think Before Your Post and Connect Safely section of the materials addresses these issues more generally.

Helpful Online Activities

- ✦ Do not lose focus on the fact that there are helpful online activities related to sexuality and relationships:
  - ‣ Find sexual health information. Districts may want to establish a page that provides links to sites with material that is accurate and appropriate for students.
  - ‣ Receive support through professional support sites.
  - ‣ Further healthy personal relationships.

Sexual Predators ~ Correct the Myths[26]

- ✦ The Crimes Against Children Research Center's research on online sexual predation has consistently found the following:[27]
  - ‣ Incidents are rare ~ Less than 1% of all arrests for sex abuse. Predators do not target children ~ they target teens. They are generally not deceptive about age and are not deceptive about intentions ~ but may pretend to love the teen. They do not track teens based on personal contact information posted online~ but do look for vulnerability and sexual interest. Violence and abduction is exceptionally rare. Teens meet with the intention to engage in sex ~ statutory rape.
- ✦ Unfortunately, all of the focus has been on dangerous adult strangers.
  - ‣ Adult family members and acquaintance sexual abusers could also use communication technologies to groom and control.
  - ‣ Teens are using are using technologies to seek sexual "hook-ups" ~ which depending on the age and initial inclinations of the parties could constitute exploitation.
    - Make sure you warn high school seniors about this, especially boys. When they turn 18, if they attempt to solicit sex with a minor they face arrest.
  - ‣ Teens are also engaging in what can only be called self-initiated child prostitution.
  - ‣ These issues are not directly addressed in the instructional material for students. There is a warning about forming relationships with those who use the Internet to seek sexual partners which is also guidance about engaging in such behaviors.
- ✦ Sexual exploiters ~ adults or older teens, strangers or not ~ target teens who are: Emotionally vulnerable. Publicly exploring sexual questions. Posting sexually provocative images. Using sexually inviting usernames. Engaging in online discussions about sex.
  - ‣ This is not "victim-blaming." To stop the harm we must address the risk behavior.
  - ‣ The grooming techniques those engaged in sexual exploitation tend to use include: Initial identification of teens who are likely targets. Relationship formation using overly friendly messages, excessive compliments, offers of assistance, and desire to be their "best friend." Sexual grooming, including offers to be a "sexual mentor," suggestions on self-stimulation, and requests for sexy pictures.

Other Risks

Fantasy Love

- ✦ Cyberdating that becomes "fantasy love."
  - ‣ Teens are pursuing personal relationships using Internet and cell phone messaging. They can easily and quickly establish unrealistic understandings and expectations because they do not have sufficient Real World interactions.
  - ‣ Both partners can get into a pattern of electronically expressing feelings of love and appreciation ~ because, for both, it is so nice to be receiving such loving messages.
  - ‣ At some time, reality may strike and one or both partners will feel betrayed. This can lead to vicious break-ups. Unfortunately, in the context of these relationships, sexual images or other material may have been shared. When the relationships break up, these images or material become ammunition to cause harm.

---

26 All of the material in this section is grounded in the research of the Crimes Against Children Research Center. This research can be found under the "Papers" link on this page: http://www.unh.edu/ccrc/internet-crimes/.

27 Wolak, J., Finkelhor, D., Mitchell, K., & Ybarra, M. (2008) Online "Predators" and their Victims: Myths, Realities and Implications for Prevention and Treatment. *American Psychologist*, 63, 111-128. http://www.unh.edu/ccrc/internet-crimes/papers.html.

- We need to help teens understand the dynamics of these online relationships so they will recognize the signs, avoid unrealistic expectations, and end relationships with understanding and kindness.

Abusive Relationships

- Abusive partners are using technologies for manipulation and control ~ especially cell phones, which provide more immediate connection.[28] Common controlling behaviors include:
  - Excessive texting to find out where the person is and who is with the person, including even hourly throughout the night.
  - Sexual harassment and sexual demands.
  - Demands for sexy nude images and then use of those images for manipulation ~ such as a threats to disseminate if the partner does not do what is demanded.
- When addressing abusive relationships teens must address use of technologies for control so they recognize and understand the signs.[29]

Sexting[30]

- Sexting is an adult term that has been applied to a range of activity. Most frequently, this is applied to the act of creating and disseminating sexy, nude images. But the term has expanded to include any use of technologies for "cyber sex." Many teens actually do not use this term.
- Two recent studies have outlined this concern.
- The MTV-Associated Press Poll – Digital Abuse Survey of 14 to 24 year olds found:[31]
  - 24% of 14 - 17 year olds reported some involvement in sexting ~ sending or receiving. (33% at the 18 to 24 age level.)
  - 10% of 14 - 24 year olds have sent a sexual image. Unfortunately, this data was not broken down into teen and young adult populations.
  - Most sent the image to a significant other or romantic interest. But 24% sent the image to someone they wanted to hook up with and 29% sent the image to someone they only knew online. Again this data is for 14 - 24 year olds.
  - Of significant concern, 61% of those who sent an image said they had been pressured by someone else to do so.
- In a national survey of those ages 12-17 who use cell phones, the Pew Internet and American Life Project ~ Teens and Sexting study found:[32]
  - 4% said they had sent sexually suggestive nude or nearly nude images of themselves to someone else via text messaging.
  - 15% said they had received sexually suggestive nude or nearly nude images.
  - Older teens are much more likely to send and receive these images; 8% of 17-year-olds had sent images and 30% had received.
  - The focus groups revealed that there are three main scenarios for sexting:
    - Exchange of images solely between two romantic partners.
    - Exchanges between partners that are shared with others outside the relationship.
    - Exchanges between people who are not yet in a relationship, but where at least one person hopes to be.
  - Anecdotally, there appears to be situations that are in the manner of the "truth or dare" games or "show me yours and I'll show you mine" interactions ~ sometimes with malicious intent.
- In a minority of these situations, this activity could involve some very serious concerns:
  - Acquisition and use of the images for malicious exploitive purposes: Demand and use by abusive partners for maintaining control. To solicit sexual "hook-ups" from other teens. As part of a pattern of juvenile sexual offending. Self-initiated child prostitution. 18 year old students who send images to minors face arrest for enticement.
- In some jurisdictions, sending nude images law enforcement has considered the creation and distribution of these images as a criminal act under laws against child pornography.
  - But these laws were enacted to prevent exploitation of minors by adults. In every jurisdiction, these statutes will need to be revised. It is not appropriate to register teens as Sex Offenders for these actions.
  - Recently, more enlightened law enforcement has taken the position that the majority of these incidents should not be viewed as criminal.
  - There is a major concern about telling teens that creating these images could be considered a criminal act. If a teen has created and sent an

---

28 Helpful statistics on this come from the Liz Clayborn site. http://www.loveisnotabuse.com/statistics.htm. Scan down the left box to Technology and TeenDating Abuse Survey, 2007.

29 The Thant's Not Cool web site, http://www.thatsnotcool.org, is a great resource.

30 CSRIU's materials on cyberbullying have been expanded to also address sexting.

31 Knowledge networks (2009) http://www.athinline.org/MTV-AP_Digital_Abuse_Study_Executive_Summary.pdf.

32 Lenhart, A. (December 19, 2009) Teens and Sexting. Pew Internet and American Life Project. http://pewresearch.org/pubs/1440/teens-sexting-text-messages.

image to someone who is now using that image in an exploitive manner, the teen will fear reporting because of the potential for prosecution. Thus fear of reporting could lead to additional exploitation and significant emotional harm. Those who use images for harmful purposes should be considered for prosecution.

- ✦ We need to strive to stop the initial behavior ~ creating and sending image ~ to ward off other harms. Focus on harm to reputation, not potential for prosecution.

Instructional Objectives

- ✦ (6-12) Students will describe how Internet resources and technologies can be used for healthy sexual and relationship purposes.
- ✦ (6-12) Students will recognize the sexual and relationship risks and describe effective strategies to prevent themselves from getting into risky situations, detect if they are at risk, and respond, including: The potential of furthering a relationship online that is not grounded in a realistic understanding of the other person. How unsafe people might use the Internet to engage in seduction for the purpose of leading to sexual involvement, common grooming techniques used by such individuals, and the emotional and health risks associated with such involvement. How abusive partners can use technologies to abuse and maintain control. That asking for, creating, or disseminating nude sexy pictures could lead to significant damage to reputation and potentially legal trouble.
- ✦ (6-12) Students will develop personal standards for how they will use technologies to form healthy personal relationships.
- ✦ (6-12) Students will recognize the potential harm to their friends from risky sexual and relationship activities, demonstrate skills in communicating to a friend how such involvement could lead to harm, and recognize the need to report such situations to a trusted adult.

About the Author

Nancy Willard, M.S., J.D. is the director of the Center for Safe and Responsible Internet Use. She 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 management of student Internet use. She has focused on issues of youth risk online and effective Internet use management since 1995. Nancy is author of two books. *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Cruelty, Threats, and Distress* (Research Press) and *Cyber-Safe Kids, Cyber-Savvy Teens, Helping Young People Use the Internet Safety and Responsibly* (Jossey Bass). Nancy’s focus is on applying research insight into youth risk and effective research-based risk prevention approaches to these new concerns.

Appendix

Intermediate, Middle, High School Lesson Plans & Other Resources

Lesson Plan 1 ~ News Story Instruction

Students will discuss issue in the context of a current news story.

- Obtain copy(ies) of news stories addressing a specific risk issue. Or ask the students to write about incidents and submit them to you - and then you can rewrite to make sure they do not include any identifying details.
- Possibly hand out the one page Cyber-Savvy Teen document addressing the risk issue.
  - Do not teach from this document. Present it simply as guidelines for how other savvy teens are making good decisions about this issue. Or just keep in mind the guidelines and in discussion help students enunciate similar guidelines.
- Divide students into small groups.
  - Ask each group to pick a situation, put themselves in the position where a close friend or a sibling has just placed him or herself at risk or is being harmed and describe what guidance they would provide to this friend or sibling and why. Use the questions set forth on page 8.
- Have each small group share insight within a larger group with the intention of developing a set of guidelines they would provide to a friend or sibling.
  - Use reflective listening and guided questions to deepen and broaden understanding. Provide positive comments to statements indicating an understanding of the potential harmful consequences and effective guidelines or problem strategies. Strive to have the students positively comment on each other's statements.

Lesson Plan 2 ~ Internet Safety Journal

Students will create a 2-page submission for an Internet safety journal. Variations: Slides presentation, poster, or blog entry.

- Page 1. Write a fictional story about a teen who gets into a risky or hurtful situation online. 250 - 300 words.
  - In the story, describe the situation, identify the people involved and describe their motivations, identify the negative consequences that occurred or were possible and the impact of these consequences on the people involved.
  - If this story is based on a real world incident that involved students in the school they should fictionalize the facts so as to protect the privacy of other students.
  - A key objective of this creative writing assignment is the focus on harmful consequences.
- Page 2. Provide guidance on how to prevent and respond to this risk situation.
  - Create a catchy saying that captures the essential guidance on how to avoid risks such as described in the story. For example: "If you wouldn't be seen like this at the mall, don't be seen like this on your profile."
  - Provide several additional guidelines in bullet format. Add a drawing, graphic image, or photo to illustrate the story.
  - Extension. Have older students make a presentation to younger students using their journal pages.

Other Great Resources

The following are organizations that provide curriculum, materials, news, and comments that meet the CSRIU requirements of being grounded in the research insight and uses effective risk prevention messaging:

- **Connect Safely, Safe Kids, Safe Teens & NetFamilyNews**. http://www.connectsafely.org/; http://www.safekids.com/; http://www.safeteens.com/; http://netfamilynews.org/ (Be sure to sign up for the NetFamilyNews. newsletter and get the RSS feeds for the blogs.)
- **Common Sense Media**. http://www.commonsensemedia.org/. (Be sure to sign up for their newsletter).
- **CyberSmart.** http://cybersmart.org/.
- **Children Online** <http://childrenonline.org/>. They have Safe Practices for Life Online curriculum - through ISTE.
- **Media Awareness Network**. http://www.media-awareness.ca.
- Federal Trade Commission **OnGuard Online**. http://www.onguardonline.gov/. (Note their great guide for parents NetCetera.)