Effectively Addressing Youth Risk Online & Youth Risk - Online

This document sets forth information and recommendations to address the risks that young people face when using interactive technologies - the Internet and cell phones - as well as the opportunity to use these technologies as a vehicle to address youth risk.

Research on Youth Online Risk

The Internet and other electronic technologies have become an integral part of the lives of children and teens. It is necessary to effectively respond to the risks associated with their use. Research has demonstrated:

- Young people who are in the greatest risk online are those at greater risk offline. They are more likely to have significant psychosocial problems, engage in offline risk taking behavior, be victims of physical or sexual abuse, engage in aggression, and have dysfunctional relations with parents or caregivers. While only a minority of youth are significantly at risk online, the repercussions are significant and must be more effectively addressed.
- Young people face significantly greater risks from known peers- not online strangers.
- Most parents are not fully involved with their child's online activities. Parents of vulnerable youth are the least likely to be effectively involved. Teens whose parents are both actively and positively involved demonstrate the lowest levels of online risky behavior. Ineffective use of "parental controls" (software solutions) can result in passive and/or negative parent involvement that can lead to increased risk.
- The majority of teens are generally making good choices online, report healthy responses to negative incidents, and are not distressed by these incidents. But even these youth are making mistakes online that could be prevented with more effective education.

Online Risk Factors

The risks young people face online are similar to the risks they face offline. However, interactive technologies can enhance these risks because of a number of factors:

- Perception of invisibility, which can lead to a reduced fear of detection which could result in punishment.
- Lack of tangible feedback that actions have caused harm to self or others.
- Material in electronic form can be widely disseminated and become permanently available.
- People can create false profiles or establish anonymity to facilitate deception and harm.
- Electronic interactions can lead to a limited-dimension perspective of others.

Youth Online Risk

Youth online risk is primarily a youth risk/mental health concern. Key areas of concern:

- Sexual Relationships & Activities. Engage in inappropriate and dangerous communications with predatory adults or teens, unsafe "fantasy" relationships, abusive use of technologies in relationships, sexual harassment, self-produced sexual images (sexting), and pornography addiction.
- Cyberbullying. Electronic aggression.
- Unsafe Communities. Provide support for self-harm actions including self-cutting, anorexia, drug use, suicide.
- Dangerous Groups. Hate groups, gangs, hacker groups, groups trafficking in pornography
- Internet Addictive Behavior. Excessive use of technologies that leads to negative repercussions.
- Unsafe Postings and Interactions. "At risk" youth more frequently post material and interact with others online in a manner that can increase the potential of harm to self and others.

Effective Risk Prevention

Research has consistently demonstrated that the "scare tactics" approach to risk prevention is ineffective. Yet the majority of Internet safety messages presented to youth and parents today transmit fear about online risks and simplistic rules against normative online behavior. Frequently, such information is not grounded in research insight.

The social norms - peer leadership approach to risk prevention is recommended. Providing the opportunity for young people to discuss these issues with each other and enunciate common protective strategies, with adult guidance when necessary, is an approach that holds much greater promise. Parents should be provided with the guidance to become more actively and positively involved in the online lives of their children.

Preventing Youth Risk - Online

The Internet provides an incredible opportunity for youth risk prevention initiatives by engaging young people where they are most active and can seek help anonymously. Online risk prevention and intervention activities can include:

- Provision of self-help information and links to resources and crisis services.
- Anonymous discussion groups and one-on-one information provision or crisis support.

Recommendations

1. Ensure a Multidisciplinary Approach - with Mental Health Professionals in a Leadership Position

A multidisciplinary approach to address these concerns is essential. Current prevention initiatives, grounded in law enforcement (Internet Crimes Against Children) and educational technology (E-Rate requirement to provide Internet safety instruction), will not result in effective prevention and intervention to what is primarily a youth risk/mental health concern. The vast majority of these concerns are not criminal in nature. Educational technology staff do not generally have expertise in youth risk prevention. Therefore, professionals in mental health and youth risk prevention must assume leadership - working in partnership with law enforcement and educational technology professionals who bring essential insight.

Because young people face greatest risks from known peers, schools must provide leadership through expanded efforts of the safe schools programs.

- At the state and local level, form a Youth Risk Online consortium that includes: mental health, safe schools, educational technology, juvenile justice, and Internet crimes professionals to collaboratively develop prevention and intervention programs and assess their effectiveness.
- In the reauthorization of Elementary and Secondary Education Act, establish a requirement that school improvement plans for both safe schools and educational technology specifically address issues of youth risk online and digital citizenship.

2. Effectively Ascertain Online Risks

There is a need for better assessment of online risks. The Center for Disease Control's Youth Risk Behavior (YRB) Survey does not address issues of youth risk online and because of timing issues will not be easy to modify.

- Develop a Youth Online Risk Behavior survey that corresponds to the YRB that would enable states to assess incident rates, risk factors, protective factors, and evaluate the effectiveness of prevention initiatives.

3. Increase Research and Translation Into Practice

Greater research is necessary to support effective initiatives.

- Increase funding for research into youth online risk. Establish better vehicles to speed the reporting of research findings and the transfer of research into practice.

4. Provide Funding for Initiatives to Address Youth Risk Online and Youth Risk Using Online Technologies

Funding to support innovative initiatives is necessary. Because youth online risk is an extension of youth risk, should be directed through Substance Abuse and Mental Health Services Agency to supports initiatives to address youth risk online. By placing the responsibility with SAMHSA, this will ensure that these efforts are effectively coordinated with other risk prevention initiatives.

- Establish a competitive grants program through SAMHSA to support national, state, and local initiatives to address youth risk online or use of online technologies to address youth risk.

5. Ensure a Reasonable Likelihood of Success of Funded Programs

There are currently no evidence-based best practices to address youth risk online. This is due to the fact that research on such risks is still emerging and the speed of change in the technologies and their adoption by youth. It is possible to establish criteria to fund initiatives that can demonstrate a substantial likelihood of success by ensuring such initiatives are grounded in current research insight and utilize effective risk prevention approaches modified to fit the realities of the online world.

- All applicants for funding through the SAMHSA program should be required to implement initiatives that meet the evidence-based best practices of the Principles of Effectiveness or follow the requirements for a waiver of Principles of Effectiveness, including:
  - A needs assessment based on objective data that describes the problems or concerns currently faced.
  - A detailed description of the implementation plan.
  - The rationale for the activity including how it is designed and why it is expected to be successful, the risk and protective factors the program is designed to address, and evidence to support that the program has a likelihood of success.
  - An evaluation plan that addresses the methods used to assess progress and how results of the evaluation and new research insight will be used to refine, improve, and strengthen the comprehensive plan.

Effectively Addressing Youth Risk Online:
An Overview

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

- Because the Internet, as well as other electronic technologies, have become an integral part of the lives of children and teens it is necessary to focus on the risks that are associated with the use of such technologies.
- More extensive professional development resources, including narrated slides presentations and handouts, are available from the Center for Safe and Responsible Internet Use, including the following titles:
  - *Cyber Safe and Savvy Students: A Guide for Educators* (for all teachers who will be addressing Internet safety issues with students).
  - *Cyberbullying & Cyberthreats: Responding to the Challenge of Electronic Aggression* (for administrators, safe school personnel and educational technology personnel).
  - *Youth Risk Online: Insight for Risk Prevention Professionals* (for safe school and mental health professionals).
  - *Web 2.0 in Schools: Effective Internet Use Management & Legal Issues.* (for administrators, educational technology professionals, and library media specialists).
- Materials are also available for parent workshops and student instruction.

A New Paradigm

Old Paradigm

- Adults understand the risks and the environment young people are interacting in.
- Adults are generally in a position to detect and intervene in situations that present risk.
- Adults impart prevention and intervention using evidence-based best practices ~ knowing that they are the authority on these risk issues.

New Paradigm

- Young people are cruising down the information superhighway with their accelerators fully engaged, but sometimes without sufficient braking power ~ while many adults are struggling to get out of first gear.
- Adults are the "immigrants" in this new cyberspace. Although we can accommodate to this new culture, we will never acculturate as well as "digital natives." Young people will reject adults who try to act like they are "authorities."
- Very frequently, the only witnesses in situations where youth are at risk online are other youth.
- There are no evidence-based best practices.

Essential Components of the New Paradigm:

- Partnership with youth ~ Work in partnership with young people ~ recognizing their greater understanding of digital culture. Avoid trying to act like an "authority."
- Empowerment of youth ~ Ensure all young people understand risks and effective protective strategies.
- Reliance on Youth ~ Enhance the ability of young people to provide assistance to peers and know when and how they should report concerns to adults.
- Continuous improvement ~ Implement approaches that are grounded in research and effective risk prevention with ongoing assessment and modification to ensure likelihood of success.
- Online engagement ~ Use online technologies to provide information, support, and intervention.

Overview of Research Findings

- Research on the risks associated with youth use of interactive technologies lead to the following understandings:[1]
  - Young people who are in the greatest risk online are the ones who are already at greater risk offline.[2]
    - They are more likely to have significant psychosocial concerns ~ including depression, anxiety, anger, and suicidal ideation ~ engage in other offline risk taking behavior, be victims of physical and sexual abuse and engage in physical and sexual aggression, have friends who are also "at risk," and have disrupted relations with parents or caregivers.
  - Young people face significantly greater risks from known peers.[3]
    - These known peers are most frequently fellow students. The online harmful interactions are closely related to, have been caused by, and can lead to, harmful interactions between students at school.
    - Thus, it is exceptionally important for schools to become actively involved in addressing these new concerns.
  - The extensive amount of fear that has been generated about young people online is not supported by the research data. In repeated studies, the majority of teens appear to be generally making good choices, report healthy responses to negative online incidents, and report that they are not distressed by these incidents.[4]
    - But the period of childhood and adolescence is a time of exploration and risk taking. Young people are making mistakes online ~ mistakes that can be more effectively prevented through effective risk-reduction education and adult involvement.
  - Parents are generally more concerned than their teens about potential online risks.[5] But unfortunately, many parents are "clueless" about their children's online activities.
    - There appears to be no correlation between the degree to which parents express concerns about online risks and their attention and supervision to their child's online activities. Thus, parent education approaches that seek to generate "fear" do not appear to be leading to greater parent involvement.

- Teens whose parents are both actively and positively involved in their children's online activities demonstrate the lowest levels of risky behavior online.[6]
- But unfortunately, the parents of the most vulnerable youth are the least likely to be effectively involved.[7]

Insight into Youth Risk Online

Electronic Aggression (Cyberbullying)

- Cyberbullying is the use of electronic technologies to engage in repeated and/or extensively disseminated acts of cruelty towards others.[8] Cyberbullying can range from minor altercations to incidents that cause devastating emotional harm.
- The different forms of cyberbullying include:
  - Flaming ~ online "fights" using electronic messages with angry and vulgar language.
  - Harassment ~ repeatedly sending offensive and insulting messages - direct bullying.
  - Denigration ~ sending or posting cruel gossip or rumors about a person to damage his or her reputation or friendships - indirect bullying.
  - Exclusion ~ intentionally excluding someone from an online group, like a "buddy list."
  - Impersonation ~ impersonating someone to make the person look bad, get that person in trouble or danger, or damage that person's reputation or friendships.
  - Cyberstalking ~ engaging in online activities that make a person afraid for her or her safety or using technology for control in an abusive dating relationship.
  - Outing ~ sharing someone's secrets or embarrassing information or images online.
  - Trickery ~ tricking someone into revealing secrets or embarrassing information, which is shared or deceiving someone online to humiliate or cause harm.
- The harm caused by cyberbullying may be greater than traditional bullying.
  - Electronic aggression can be exceptionally vicious, there is no escape for the target, the harmful materials distributed more widely, the aggressor can remain anonymous, and the incidents can involve large numbers of others.
  - Cyberbullying is resulting in school failure, school avoidance, violence, and suicide.
- Students are also targeting school staff online. Students who are happy and feel connected to their school community are not generally targeting staff online.
  - Material could range from nasty harmful material, convenient target, anguish of a student whose learning or social challenges are not being met, retaliation to staff abuse, or legitimate political protest.
- A review of emerging research on cyberbullying leads to the following insight:[9]
  - Cyberbullying is a significant concern for young people. But the incident rates of cyberbullying reported in the research appear to be related to how the questions are asked. Most surveys are not yet effectively distinguishing between minor and significant incidents.
  - The continuing incidents between known peers are causing the highest degree of distress. Addressing these incidents will be challenging. These incidents will impact schools because they appear to be related to on-campus bullying or could lead to retaliation at school. A significant portion of incidents appear to involve online retaliation against the person who has been aggressive.
  - Both aggressors and targets appear to present significant psychosocial concerns and report involvement in offline aggression ~ which is more likely to occur where they are physically together at school. They also have disrupted relations with parents ~ which means schools will be less able to rely on parents for effective supervision, prevention and response.
  - The vast majority of young people are not reporting these incidents to adults. The primary reason reported for this is that young people have or feel they should be able to handle the situation on their own ~ which is something we should encourage. But many say they do not tell for fear of getting into trouble or losing Internet access. This may, in some cases, be a legitimate concern because their hurtful actions ~ online or in the real world ~ may be part of the problem.

Risky Sexual & Relationships Activities

- Teens are maturing sexually and engaging in a range of sexual and personal relationship-related activities online. Much of this can be very positive. Risks include:
- Online Sexual Predation.
  - Much of what people think they know about online sexual predation is not supported by the research.[10] These incidents are very rare ~ just 1% of arrests for sexual abuse. Predators are not targeting children. Deception about age and sexual intention is rare, however, deceptive promises of love does occur. Abduction or violence is rare. Predators are not tracking teens based on personal contact information and abducting them. Teens meet with the predators knowing they are adults and intending to engage in sex ~ many times they meet on more than one occasion.
  - The teens who are at greatest risk of online sexual exploitation ~ by adults or teens, strangers or not ~ are those who are emotionally vulnerable, exploring sexual questions in unsafe forums, posting sexy images, and using sexy usernames. Boys, likely those questioning their sexual orientation, are also at risk.[11]
- Pedophiles Online ~ Child Pornography.
  - Family or acquaintance abusers are using technologies for grooming or the creation of pornography. Pedophiles are also engaging with others in online communities where they rationalize their sexual activities and share child pornography.[12] The risks of sexual abuse by someone trafficking in child pornography are high.
    - Warning signs are addictive access, excessive secrecy, expensive equipment with no logical reason.
- Cyberdating or Fantasy Love.
  - Cyberdating is, and will continue to be, a very common way for teens to form and develop relationships and can be very healthy.
  - Teens might develop a "fantasy love" relationship with someone online that is based on significant misperceptions and engaging in "cybersex" with images retained and distributed or threat of distribution.
- Abusive Relationships.
  - Teens in abusive dating relationships are being controlled, threatened, and humiliated by the controlling partner through cell phones and the Internet.[13]

- The controlling behavior includes spreading rumors, demanding, sharing or threatening to share private or embarrassing images, excessive text messaging to maintain control over activities and relationships.

- Self-Produced Nude Sexy Images ~ Sexting.
  - Teens are self-producing and distributing nude sexual images, frequently via cell phone.
    - Laws against the production and dissemination for child pornography were enacted to prevent minors from being abused by adults. The application of these laws presents significant concern.
    - This activity is frequently "courtship ritual" behavior. But could also be in the context of abusive partnerships or self-initiated prostitution.
- Online Pornography.
  - Teens may intentionally or accidentally access online pornography.[14] Most teens, especially boys, will spend some time looking. The teens at risk are the ones who do so excessively or are attracted to child pornography.

Cyberthreats Online Threats & "Leakage"

- Cyberthreats include direct threats or distressing material that raises concerns the person is emotionally distraught and may be considering harming someone, harming him or herself, or committing suicide.
  - Young people make threats all the time. Their tone of voice, posture, overall interaction allow others to determine if it is a "real threat." Sometimes online material that looks threatening is just a joke. However, online threatening material can be very real.
- The Federal Bureau of Investigation calls this kind of material "leakage." When a young person intentionally or unintentionally reveals clues to feelings, thoughts, fantasies, attitudes, or intentions that may signal an impending violent act against self or others.[15] Assume they will post this kind of material online

Unsafe Communities & Dangerous Groups

- Online "communities" and web sites support unsafe activities or encourage dangerous activities.
  - Unsafe communities support actions that can cause self-harm, including self-cutting, anorexia and bulimia, steroid use, drug use, passing-out games, suicide, and other similar unsafe activities.[16]
  - Dangerous groups promote actions that could cause harm to others, including hate sites and groups, gangs, and other troublesome groups including groups of local youth, hacker communities, groups that exchange pornography and discuss pedophilia.[17]
- These groups all appear to have similar features:
  - Strong emotional support for marginalized youth where participants act as "mentors."
  - Symbols that foster group identity.
  - Online rituals that solicit evidence that the participant is truly committed to the ideals of the group.
  - Practices of exclusion of anyone deemed not to abide by the group norms ~ which will act to reinforce the importance of abiding by those norms to remain connected and receive support.
  - Naturalizing/rationalizing the injurious self-harm or aggressive values or behavior.
- Not all online communities that vulnerable teens participate in are harmful. Marginalized youth may find a very healthy online environment where they fit in with people who have their own interests.[18]
- It is simply not possible to get rid of the harmful groups or try to cut off a teen's access. But because marginalized youth are attracted to online groups, the provision of online support services to such youth represents a largely untapped area of potential intervention.[19]

Posting Material, Interacting With Others, Balancing Life Activities

- Underlying all of the above risks are three foundational concerns. Vulnerable youth may be more apt to engage in online behavior that is more likely to lead them into dangerous situations.
- They may post material online, such as sexualized images, and engage in unsafe communications with others, such as discussing sexual issues with online strangers.[20]
  - The issue is not that they are posting personal information or interacting with strangers online, which is normative online behavior. But the manner in which they are engaging in such online behaviors can place them at greater risk.
- Addictive access is an excessive amount of time spent online resulting in lack of healthy engagement in other areas of life. The research on time spent involved with electronic technologies and psychosocial concerns is somewhat mixed.
  - Some research has indicated that young people who are very active online are also very engaged in school and other activities ~ "highly social" young people.[21]
  - Other research has shown a connection between an excessive amount of electronic activity and depression, social anxiety, and suicidal ideation.[22] The American Psychiatric Association recently noted that Internet addiction appears to be a common disorder that merits inclusion in the Diagnostic and Statistical Manual of Mental Disorders.[23]

Influences on Online Behavior[24]

You Can't See Me ~ Perception of Invisibility

- 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.

I Can't See You ~ Lack of Tangible Feedback

- No tangible feedback about consequences of online activities. Can interfere with recognition of harm and feelings of remorse. Focus their attention on harmful consequences.

Didn't Think ~ Brain Development

- 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. Empower teens to independently make good choices.

Who Am I? ~ Exploration of Identity

- 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? ~ Maturing Sexuality

- 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 ~ Ability = Right

- They may forget that Real World values should control their online choices. They think if they can do something, it is okay. Tell them, "Just because you can, doesn't make it right."

Everybody Does It ~ Online Social Norms

- They may follow others who make inappropriate choices. Watch out for "friends." Tell them, "Just because they do it, doesn't make it right."

How Far Can I Go? ~ Limit Testing

- Teens test limits. This how they learn about boundaries. Discuss risks. Do not overreact to mistakes. Respond with an appropriate consequence.

Doing What They Say ~ Social manipulation

- Others seek to manipulate them. Offer "online candy." Seek commitment to special relationship or a group. Teach them to recognize attempted manipulation.

Looking for Love ~ Vulnerable Youth

- 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.

Technopanic & Fear-Based Messages

- 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.[25] It is essential that we neither ignore, nor exaggerate the risks.
  - Conveyed by some media, politicians, organizations, and companies ~ often with other motivations.
  - Related to the profound changes society is going through ~ challenging social "authority."
- The harms caused by technopanic are that young people are less likely to:
  - Be receptive to accurate guidance delivered by adults ~ because they don't think adults understand.
  - Report online concerns to adults ~ because they think adults will overreact.
- Many of the current Internet safety messages and recommended approaches are not supported by the research on effective risk prevention. The ineffective approaches include:
  - Fear-based information ~ not grounded in research.
  - Stranger danger warnings.
  - Simplistic rules against normative online behavior that is not inherently risky.
  - The only guidance on how to respond is to tell an adult.
  - Authoritarian delivery of instruction by adults who lack credibility because they don't understand digital culture.
  - Encourage reliance parental controls, including filtering and monitoring software.

Effective Prevention

- It is necessary to keep children in safe places and prepare teens to make good choices in the digital world.

Social Norms Approach

- The social norms approach to risk prevention is strongly recommended.[26]
  - This approach should correct negative misperceptions that a majority of young people are engaging in risky or irresponsible online behavior and identify, model, and promote the healthy, protective behaviors that are the actual norm.[27]

Risk Factors Related to Technology

- Many of online risk issues are an extension of risky behavior into the online environment ~ vulnerable youth using technologies. However, there are specific technology-related aspects to this behavior:
  - Youth are providing material in permanent electronic form that can then be used to harm them.
  - Technologies provide the ability to create a "false persona" (false image) or "fake profile" (pretend to be someone else) ~ resulting in deception and harm.
  - Young people are interacting with people online who are not known in the real world ~ who could not be "real," become hurtful, or seek to involve the young person in unsafe or dangerous activities.
  - Electronic communications allow for a much wider range of dissemination of harmful material ~ thus a single incident can cause greater emotional harm.
  - Online interactions can lead to a limited-dimensional perspective of people ~ thus resulting in fantasy perceptions about someone that are not real.
  - Electronic communications allow teens with lower "social power" to more safely engage in online harm directed at others ~ frequently retaliation against those who have caused harm to them in the real world.
  - Electronic communications allow for the involvement of many. Teens are functioning as members of extensive social networks that can become involved in inflicting harm or encouraging risky attitudes and behavior.

Protective Factors

- The key protective factors within the technology environment appear to include:
  - In Web 2.0 environments, online interactions are often quite visible and recorded in electronic form ~ which allows for more effective detection, investigation, and intervention.
    - This "real" evidence can be used to more effectively understand critical risk factors and to rebut denial.
  - Young people are in a position to detect concerns and influence others. The young people who are at risk online are not invisible to their peers. Thus, a peer leadership approach to risk prevention is likely to be very effective.
  - Because vulnerable youth are seeking information and connections online because they can be anonymous in

doing so. Risk prevention specialists can use the online medium to more effectively engage these youth ~ through online information, discussion groups, and electronic crisis intervention.

Effective Protection and Instruction

- The primary protection for children is through parental attention to the kinds of sites they access and people they communicate with, along with simple rules related to the places they can go, people they can communicate with, kinds of personal information they share, and how to respond to hurtful or uncomfortable situations.
  - Parents must be encouraged to establish "fenced play yards" online. Technologies can assist with this.
- For teens, the focus must shift to empowerment by helping teens recognize the risks and learn effective strategies to prevent themselves from risk, detect if they are at risk, and effectively respond, including when they should request assistance from an adult.
  - Focus on potential harmful consequences using real world examples that accurately illustrate the concern.
  - Help them gain effective problem-solving skills.
  - Help them understand the traps that can lead them to make bad choices online and how to evaluate the options to make good choices.
  - Encourage teens to be leaders within their digital online community.
  - Avoid lecturing to students. Set up situations where students discuss these issues, allowing the more savvy students to take the lead in suggesting protective strategies. The role of the teacher is to ask guided questions to deepen understandings.
- Encourage parents to be actively and positively involved in what their child is doing online, engage in respectful monitoring, avoid any overreaction if their child ever report an online concern, and to encourage their child to help others and report online concerns.

Cyber-Savvy Teens

- 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 risk, 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 others and the digital community.
  - They help others online.
  - They report concerns to a responsible adult or site.
  - They promote digital civility.

Legal Issues Related to School Intervention

Free Speech v. Student Safety

- The challenge ~ the balance ~ the bottom line.
  - The more harmful incidents of online aggression occur when students post harmful material while off-campus ~ because this is where they have more unsupervised use. But the harmful impact is at school ~ because this is where students are physically together.
  - Students have important free speech rights.
  - School officials have an important obligation to ensure the safety of students and the delivery of instruction.
  - Regardless of where the speech occurs, when the impact is at school and jeopardizes the safety and well-being of students or the delivery of instruction, school officials must respond to protect the rights of other students.
  - But in a significant number of Internet situations, a formal disciplinary response will either be entirely ineffective ~ or create greater problems.
- Cases addressing school response to off-campus student speech have indicated that school officials have the authority to formally respond to off-campus speech if that speech has created, or a reasonable person would perceive it could create, a substantial disruption at school or interference with the rights of students to be secure.[28]
  - But school officials may not respond based on disapproval of the content or manner of the speech, however offensive, or the perspective that the student's speech is inconsistent with educational standards.

Requirements to Respond to Off-Campus Speech That Targets Students[29]

- School "nexus." A nexus between the off-campus online speech and the school community.
  - Speech involves students or staff or is in some other manner connected to the school community.
- Impact at school. The impact has, or it is reasonably foreseeable it will be, at school.
  - "School" includes school-sponsored field trips, extracurricular activities, sporting events, and transit to and from school or such activities.
- Reasonably foreseeable. School officials must be able to point to a specific and particularized reason why they anticipate a substantial disruption or interference ~ not mere apprehension of the possibility of a disruption.
  - Timing is an issue. Formal response is for the purpose of preventing an imminent foreseeable substantial disruption or interference ~ not after the fact because a disruption could possibly have occurred, but did not.
- Material and substantial impact. The impact has, or it is reasonably foreseeable it will be, significant.
  - Not anger or annoyance. Not disapproval of the expression of a controversial opinion. Not simply a situation that requires investigation.
- Disruption of school or interference with rights of students. The speech has caused, or it is reasonably foreseeable it will, cause:[30]
  - Significant interference with instructional activities, school activities, or school operations.
  - Physical or verbal violent altercations.
  - A hostile environment for any student that impairs that student's ability to participate in educational programs or school activities.
- Hostile Environment[31]
  - Assess hostile environment based on target's subjective response and a reasonable observer perspective.

- Causal relationship.
  - The speech has been, or it is reasonably foreseeable it will be, the actual cause of the disruption. Not some other factor, such as administrator reaction.

Off-Campus Speech that Targets School Staff or Challenges School Policy

- Likely will not meet substantial disruption standard ~ unless speech has, or it is reasonably foreseeable it will, cause a significant interference with the delivery of instruction, school activities, or operations.
  - Under the First Amendment students have the right to protest school policies and the actions of school staff.
  - But truly harmful speech could provide the basis for a civil law suit ~ which will provide greater deterrence.

Potential Threat

- School officials have clear authority to respond to online material that raises a concern that a student may pose a threat to self or others.[32]
  - Ask: Does the student POSE a threat, not did the student POST a threat? Has this online material been posted in retaliation for unresolved conflict or abuse the poster has been subjected to at school?

Responding to On-Campus Speech

- School officials have the authority and responsibility to respond to any harmful or inappropriate speech through the District Internet system.
  - This includes material that has or could create a substantial disruption or material that is offensive and contrary to school's mission.
- School officials can impose educationally based standards on student material posted publicly on district web pages.[33]
  - But state student free press statutes will impact this.[34]
- School officials have the authority and responsibility to respond to any harmful speech that takes place while students are using cell phones or other personal digital device on-campus.
  - But searching a student's cell phone or PDA without parent permission may violate state wiretapping laws. Legal standards are unclear ~ check with school counsel.[35]
  - School officials may also find nude images, which could be considered child pornography. Do not provide to anyone other than the police. That could be considered distributing child pornography ~ a crime!

Liability for Hostile Environment

- School officials likely have the responsibility to respond to off-campus online speech that has created a hostile environment at school for a protected student, if they know of the concern ~ because they clearly do have the authority to respond if a hostile environment has been created for a student on-campus.[36]
  - School officials definitely have a responsibility to respond if there are on-campus harmful interactions that are associated with off-campus online harm.
  - Failure to investigate and respond because of the misperception that this is "off-campus, not my job" could constitute "deliberate indifference" and lead to liability.

Other Legal Issues Related to Web 2.0 in Schools

- Student privacy and FERPA.
- School staff online.
- Free speech ~ access, post, academic freedom.
- Disability access.
- Copyright.
- Publishing torts ~ hostile environment.
- Liability prevention practices for schools.

Investigation & Intervention

- Many of these situations will involve some form of online aggression. Others situations will involve a student who is placing himself or herself at risk online.

Set the Stage

- Establish a response team that includes safe school and educational technology personnel.
- Make sure students can easily report anonymously and make a commitment to confidentiality.
- Make sure that all response team members can quickly override the filter to investigate.
  - This is not a violation of the Children's Internet Protection Act and is essential to protect student safety.

Investigation

- Gather and preserve all electronic evidence.
- Determine identities
- Review the situation ~ looking for underlying vulnerabilities and contributing factors.

Intervening

- Imminent Threat.
  - If the speech appears to present an imminent threat, contact law enforcement and initiate a protective response. Watch out for all of the possible alternatives. This could just be a joke.
- Suspension.
  - Avoid the "suspension" response unless there are school safety reasons to temporarily remove a student from the school environment. Suspensions are often ineffective and can lead to more extensive online retaliation.
- Take-down.
  - Once the materials have been preserved, get them taken down as rapidly as possible. Look for the abuse report or complaint feature on the home page of the site.
- Discussions with Target(s) in Aggression Situations.
  - Must seek to address the underlying problems that are leading to unhealthy personal relationships and identify a remedy that the target thinks will be effective.
  - Provide invisible assistance. In some situations it may be far more effective for a counselor to work with a target of online aggression to help that target respond in a strong manner.
- Discussions with Aggressor(s).
  - The primary objective is to get students to the point of feeling remorse, shame, and a desire to remedy and discontinue the harm ~ not anger. Focus on restorative justice.
  - Pay attention to the underlying reasons why the aggressor is engaging in harmful behavior.
- Discussions with Students Placing Themselves at Risk.

- If the student has not thought things through, intervention may simply require confronting the student with evidence ~ thus demonstrating that nothing posted online is private ~ and discussing the risks, appropriate responses to try to remedy the harm, and guidelines for effective responses in the future.
- If the risk behavior provides indications of greater vulnerability, professional intervention will be necessary.

Comprehensive Prevention Approach

Research-Grounded

- This approach is grounded in research, modified to reflect new technology environment, and contains the elements necessary to have a reasonable likelihood of success and achieve a waiver of the Principles of Effectiveness requirement.
  - This approach is not an evidence-based best practice because the research on online risk is still emerging and the technologies and challenges continue to change.

Social Intelligence

- The foundation for addressing Internet safety and youth risk online is helping students gain effective social and personal relationship understandings and skills. Schools are strongly advised to have in place a strong program to support social intelligence, positive social and relationship development, and youth leadership.
  - Provide support for positive behavior.
  - Strengthen skills in empathy.
  - Impart skills in interpersonal relationship problem-solving.
  - Engage bystanders in prevention.
  - Train students in peer mediation.

Systemic Change in Organizational Structure.

- Establish a collaborative Youth Risk Online group involving safe school and educational technology professionals to address youth risk online issues.
  - At the secondary level, involve students in all aspects of planning ~ including policy development.
  - Interface with local law enforcement, especially to address procedures related to sexual exploitation, "sexting," online threats, and dangerous online groups.

Needs Assessment

- Conduct a formal or informal needs assessment to provide insight into the extent of the local problem and to support evaluation.

Threat Assessment

- Threat assessment protocols and suicide prevention plans MUST be revised to incorporate the reality that significant amount of teen communication related to threats and suicide will be occurring online!

Policy and Practice Review

- Bypass Internet filter.
- Cyberbullying.
- Cell phone.
- Personal imaging device.
- Extracurricular activities.

Internet Use Management

- There are significant issues that must be addressed about effective management of Internet use.
  - Overreliance on filtering, which students can bypass.
  - Ineffective supervision and monitoring practices.
  - Essential to incorporate Web 2.0 communication technologies into instruction.
- Implement effective Internet management approach.
  - Focus on educational purpose and activities.
  - Controlled online instruction environments.
  - Increased technical monitoring.
  - Effective filter management.
  - Use Web 2.0-based instruction to address digital citizenship and responsible publishing.

Professional Development

- Implement a "triage" approach to address professional development based on responsibilities.

Parent Outreach

- Provide information on how to prevent, detect and intervene if their child is victimized online, prevent their child from engaging in harmful online behavior, empower their child to be a responsible bystander/peer leader.
  - Provide information to parents through general information in newsletters, parent workshops, and "just-in-time" resources.

Community Outreach

- Provide information and training to mental health and law enforcement professionals, community and youth organizations, and media.

Student Education

- Provide guidance to students on risks and protective strategies using the instructional approaches described above.

Evaluation and Assessment

- Use a continuous improvement model. Must constantly evaluate and modify based on new insight and results of local efforts.
  - Specifically evaluate the effectiveness of school investigation and intervention. Students will not report if they do not perceive this will resolve the problem.

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. 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 of youth risk online. © 2009 Nancy Willard. Permission to reproduce and distribute for non-profit purposes. Email: nwillard@csriu.org ~ Website: http://csriu.org.

References

1 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. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_C_TF_Project_Plan.pdf.

2 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; The December 2007 Supplement of the *Journal of Adolescent Health*, Youth Violence and Electronic Media: Similar Behaviors, Different Venues? http://www.jahonline.org/content/suppl07 contains several articles that document the association of psychosocial concerns and cyberbullying.

3 Wolak, J., Mitchell, K., and Finkelhor, D. (2006). Online victimization of youth: Five years later. *National Center for Missing & Exploited Children Bulletin* - #07-06-025. Alexandria, VA. http://www.unh.edu/ccrc/internet-crimes/papers.html; McQuade, S. (2008) *Study of Internet and At Risk Behaviors*; http://www.prweb.com/releases/Cyber_Safety/Ethics_Initiative/prweb1035784.htm.

4 All of the studies cited in this section.

5 Rosen, L. D., et al., (2008) The association of parenting style and child age with parental limit setting and adolescent MySpace behavior, *Journal of Applied Developmental Psychology*. doi:10.1016/j.appdev.2008.07.005.

6 Rosen based his analysis on the types of parenting originally identified by Diane Baumrind. Authoritative parents are active and positive.

7 Wolak (2008).

8 Willard, N.E. (2006) *Cyberbullying and CyberThreats: Responding to the Challenge of Online Aggression, Threats, and Distress*. Research Press.

9 All articles in December 2007 Supplement. http://www.jahonline.org/content/suppl07. Hinduja, S. & Patchin, J. W. (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Sage Publications (Corwin Press) Juvonen, J. & Gross, E. (2008) Extending the school grounds?--Bullying experiences in cyberspace. *Journal of School Health*. Vol. 78, Issue 9, p 496. http://www3.interscience.wiley.com/journal/121371836/abstract?

10 Wolak (2008); Wolak, J., Finklehor, D., & Mitchel, K.(2009) *Trends in Arrests of "Online Predators," Crimes Against Children Research Center*.. Currently on home page: http://www.unh.edu/ccrc/. will be moved to: http://www.unh.edu/ccrc/internet-crimes/papers.html.

11 Wolak (2008).

12 Eichenwald, Kurt, (August 21, 2006) From Their Own Online World, Pedophiles Extend Their Reach. *New York Times*.

13 Picard, P. (2007) *Tech Abuse in Teen Relationships Study*. Liz Claiborne Inc. http://www.loveisnotabuse.com/surveyresults_2007mstr.htm.

14 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/internet-crimes/papers.html.

15 O'Toole, M.E. (1998) *The School Shooter: A Threat Assessment Perspective*. Federal Bureau of Investigation. http://www.fbi.gov/filelink.html?file=/publications/school/school2.pdf.

16 Whitlock, J.L., Powers, J.L., Eckenrode, J., 2006. The virtual cutting edge: the Internet and adolescent self-injury. *Developmental. Psychology*. 42(3), 407–417;, Mitchell, K. & Ybarra, M. (2007). Online behavior of youth who engage in self-harm provides clues for preventive intervention. *Preventive Medicine*, 45: 392-396. http://www.unh.edu/ccrc/internet-crimes/papers.html; Pascoe, C.J.. 2008. *"You're Just Another Fatty:" Creating a Pro-Ana Subculture Online*. Digital Youth Research http://digitalyouth.ischool.berkeley.edu/node/104. January 22, 2008.

17 Chau, M., & Xu, Jennifer. (2007). Mining communities and their relationships in blogs: A study of online hate groups. *International Journal of Human-Computer Studies*, 65(1), 57-70; Southern Poverty Law Center. (2004). *Hate Groups, Militias on Rise as Extremists Stage Comeback*. http://www.splcenter.org/center/splcreport/article.jsp?aid=71; National Alliance of Gang Investigators Associations. *2005 National Gang Threat Assessment*. http://www.nagia.org/PDFs/2005_national_gang_threat_assessment.pdf.

18 Ito, M., Horst, H., Bittanti, M., boyd, d., Herr-Stephenson, B., Lange, P., Pascoe, C.J., and Robinson, L (2008), *White Paper - Living and Learning with New Media: Summary of Findings from the Digital Youth Project*. http://digitalyouth.ischool.berkeley.edu/report.

19 Mitchell, K. & Ybarra, M (2007).

20 Ybarra, M., Mitchell, K., Finkelhor, D., and Wolak, J. (2007). Internet prevention messages: Targeting the right online behaviors. Archives of Pediatrics & Adolescent Medicine, 161: 138-145. http://www.unh.edu/ccrc/internet-crimes/papers.html.

21 Lenhart, 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.

22 Kim, K., Ryu, E. Chon, M., Yeun, E., Choi, S.,, Seo, J., Nam, B. (2006) Internet addiction in Korean adolescents and its relation to depression and suicidal ideation: A questionnaire survey International. *Journal of Nursing Studies*, 43, 185–192. (The levels of depression and suicide ideation were highest in the Internet-addicts group.); Jenaro, C., Flores, N., Mez-vela, M., Gonza, F., Gil, L., Caballo, C. (2007) Problematic internet and cell-phone use: Psychological, behavioral, and health correlates, *Addiction Research and Theory*. 15(3): 309–320 (Heavy Internet use is associated with high anxiety; high cell-phone use is associated to being female, and having high anxiety and insomnia.).

23 Block, J.J. (2008) Issues for DSM-V: Internet Addiction, *Am J Psychiatry* 165:306-307, doi: 10.1176/appi.ajp.2007.07101556, http://ajp.psychiatryonline.org/cgi/content/full/165/3/306.

24 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.

25 Roush, W. (2006) The Moral Panic Over Social Networking Sites. *Technology Review*. http://www.technologyreview.com/communications/17266/?a=f. See also, Cohen, S. (1972). *Folk devils and moral panics: the creation of the Mods and Rockers*. London: MacGibbon and Kee.

26 DARE is now implementing the Keepin it REAL drug prevention curriculum. This curriculum has demonstrated its effectiveness. The approach taken in the KiR curriculum is very similar to the approach that is recommended in this document. http://keepinitreal.asu.edu/kir-curriculum.

27 http://www.socialnorms.org.

28 *Layshock v. Hermitage Sch. Dist.*, No. 06-116 (July 10, 2007), relying on ruling in *Tinker v. Des Moines*, 393 U.S. 503, 507 (1969).

29 These requirements come primarily from the well-reasoned *Layshock* decision.

30 This is based on an in-depth analysis of cases involving both on and off-campus speech that have been decided under *Tinker*. An extensive analysis is available from CSRIU.

31 *Saxe v. State College Area School District*, 240 F.3d 200 (3rd Cir. 2001).

32 Sarah E. Redfield, Threats Made, Threats Posed: School and Judicial Analysis in Need of Redirection, 2003 *BYU EDUC. & L.J.* 663.

33 *Hazelwood v. Kuhlmeier*, 484 U.S. 260 (1988).

34 Understanding student free-expression laws: Renewed push to pass state laws as courts chip away at First Amendment rights in schools. http://www.splc.org/report_detail.asp?id=1351&edition=43.

35 *Klump v. Nazareth Area Sch. Dist.*, 425 F. Supp. 2d 622, 641-42 (E.D. Pa. 2006).

36 *Davis v. Monroe Bd. of Educ.*, 526 U.S. 629 (1999).