The majority of young people make positive choices online, effectively respond to the negative situations that do occur, and are not overly distressed by these situations. They may make mistakes that could be prevented through better education. A minority of young people face greater risks that must be addressed through effective prevention and intervention.

The Protecting Children in the 21st Century Act added a provision to the Children’s Internet Protection Act (CIPA) requiring that schools receiving E-Rate and other technology funds provide instruction in Internet safety. On August 11, 2011, the Federal Communications Commission issued regulations on this act. Under these regulations, districts must have an Internet safety policy that meets the following requirement:

This Internet safety policy must also include monitoring the online activities of minors and must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

A school, school board, school district, local education agency, or other administrative authority of a school receiving E-rate funding for Internet access and internal connections must certify on its FCC Form 486 or FCC Form 479, beginning with funding year 2012 (July 2012), that it has updated its Internet safety policy. Schools do not need to issue an additional public notice and hold a hearing in order to update their policies.

The FCC specifically declined to define or interpret the terms provided in the new statutory language, such as “social networking” or “cyberbullying.” In addition, the FCC indicated that it would not detail specific procedures or curriculum for schools to use in educating students about appropriate online behavior because, in its opinion, these are determinations that are better be made by schools.

Effective Internet Safety Education

A Family Online Safety Institute discussion paper, Increasing Youth Safety and Responsible Behavior Online: Putting in Place Programs that Work, written by Lisa M. Jones and David Finklehor of the Crimes Against Children Research Center presented the following concerns about current Internet curriculum:

Hundreds of programs are being developed to promote safe and responsible online behavior among youth. They are being successfully marketed and eagerly adopted because of their appealing content, exciting graphics, engaging games, catchy phrases and cool characters. But that is not enough. The bottom line for everyone to remember -- funders, program developers, communities, schools, and families -- is that these programs need to actually work. They need to change youth attitudes and inspire youth to make smart and ethical choices about how they behave online. If programs are not doing this, then no matter how beautiful the graphics or sophisticated the video production, time and money are being wasted. Children are not safer and parents and teachers may wrongly conclude that they have successfully addressed the problems.

Jones and Finklehor call attention to the importance of ensuring that curriculum programs are effective through scientific evaluations. This is challenging. There are currently no evidence-based best practices in this area. Youth behavior when using digital technologies is a new phenomenon that has not been extensively studied. Strategies to positively influence digital behavior are not fully understood. Conducting an evaluation is difficult when insight is still emerging. Further, such evaluations require time and resources. But under Protecting Children in the 21st Century Act, schools must provide instruction starting in 2012.

What can and should schools do to ensure a likelihood of success in the delivery of Internet safety instruction?

Cyber Savvy Strategy

Nancy Willard’s new book, Cyber Savvy: Embracing Digital Safety and Civility, provides comprehensive insight for educators to provide instruction. Her focus is on ensuring young people become Cyber Savvy. Cyber Savvy youth:

- Keep Themselves Safe. They understand the risks and they know how to avoid getting into risky situations, to detect whether they are at risk, and to effectively respond.
- Present a Positive Image. They present themselves online as someone who make positive choices.
- Respect Others. They respect the rights, privacy, and property of others and treat others with civility.
- Take Responsibility for the Well-being of Others. They help others and report serious concerns to a responsible adult.

Instructional Components

Incorporate these three key components into instruction:

- Reinforce Positive Norms. Universal education must promote the positive norms and effective practices held by the majority of the students. This can be accomplished through student-led constructive instruction, use of older students to teach younger students, and messaging about making positive choices.
- Strengthen Effective Skills. Constructive instruction can also help students gain skills through sharing of effective practices and strategies. Effective skills include problem-solving and decision-making. Students must also recognize possible negative influences related to the use of technologies, as well as the influences for making positive choices.
- Encourage Helpful Allies. As helpful allies, young people can provide support to a peer who is at risk or being harmed, challenge irresponsible or hurtful behavior, and report unresolved or serious concerns. Increase skills in responding and emphasize the positive perspective of helpful allies.

Key School Action Steps

Implement these key actions steps:

- Establish a Multidisciplinary Coordinating Committee. Include educational technology specialists, school librarians, and health teachers—and the school resource officer if this person will be providing instruction. Collaborative involvement of these professionals is essential.
- Ensure Professional Development. All members of this team require an understanding of the issues and effective instructional approaches that is grounded in research insight. A significant amount of disinformation has been disseminated over the last decade about Internet risk. Fear-based messaging and simplistic rules against normative online behavior will not be effective in preventing risk behavior.
Use Local Survey Data

Embracing Digital Youth has developed, and is currently pilot testing, an online survey for 7th to 12th grade students that assesses the following:

- Norms and practices around use of digital technologies including practices on social networking sites, posting information, establishing friendship links, and time spent online.
- Norms and practices around issues of aggression and other risks, with a special focus on the role of witnesses.
- Incident data, as well as risks and protective factors related to situations involving digital aggression, abuse, and exploitation.

This survey will be available to schools for three purposes:

- Planning and Needs Assessment. The survey is designed to provide insight into norms and practices, as well as risk and protective factors. This will enable school leaders to more fully understand the challenges their students are facing, as well as how effectively many students are making choices. Based on this insight, schools can develop measurable objectives.
- Instruction and Messaging. The data can provide the basis for highly interactive classroom positive norms instruction and messaging. By demonstrating that the majority of students make positive choices, do not like to see others harmed or at risk, and think very highly of those students who step in to help, the minority of students who are not making good choices will be more likely to emulate their peers. The use of “real” data from their classmates should be highly influential.
- Evaluation. Repeated use of this survey will allow the district to ascertain whether their instructional and prevention approach is changing students’ attitudes and behavior. This will provide school officials with a vehicle to ensure accountability.

Evaluating Curriculum or Presenters

While some schools may develop their own instructional resources, others may choose curriculum or invite presenters to talk with the students. Carefully consider the potential effectiveness of curriculum or presenters:

- Determine the organization or individual’s underlying area of professional expertise.
- Request information on the research insight and risk-prevention approach that has been relied on in creating the curriculum or developing the presentation.
- Evaluate the curriculum to determine whether it uses any of the following problematical approaches. Ask presenters for references for past presentations and make inquiries related to these issues.

Don’ts & Do’s

The following are approaches to avoid and alternatives to look for when evaluating curriculum or presenters:

- Avoid approaches that communicate the misperception that many young people are at risk online or are engaging in unsafe or irresponsible actions. Choose approaches that communicate positive messages that the majority of young people make safe and responsible decisions and effectively respond to negative situations.
- Avoid approaches that impart inaccurate, fear-based information and messaging. Choose approaches that provide insight grounded in research on actual risks and degree of harm associated with those risks.
- Avoid approaches that impart simplistic rules against normative online behavior like rules against communicating with any onlineistrangers or posting photos of oneself or of friends online. Choose approaches that focus on problem solving and skill building.
- Avoid approaches that impart “stranger danger” warnings and try to make it appear that anyone they meet online is highly likely to want to harm them. Choose approaches that focus on strategies young people can use to safely interact online with people who are known in person or not.

- Avoid approaches that rely primarily on adults directly instructing secondary students. However, sometimes this approach can be useful, for example, having a law enforcement official make a special presentation. Create situations where the majority of the instruction engages students in talking with their peers.
- Avoid having students sign “Internet safety pledges.” Encourage students to develop their own statements of personal standards.
- Avoid recommending that parents of teens strongly rely on filtering or monitoring technologies. Recommend that parents engage in active and positive interactions, use protective technologies for children, and constructively use monitoring technologies for tweens and at-risk teens.

Law Officers as Instructors

Law officers can provide important insight for students about when digital behavior crosses the line to become a criminal act. This is important from both the perspective of student victimization, as well as engaging in criminal behavior. Criminal concerns include: child pornography, sexual exploitation or trafficking, criminal aggression, cyberstalking, online threats, and online gang activity.

Law officers will be most effective if they reinforce students’ positive norms and focus their attention on the importance of recognizing and reporting serious concerns to a responsible adult.

Cyber Savvy

The following are the key issues addressed in Cyber Savvy: Embracing Digital Safety and Civility:

- Avoid the Impulse. Remember, what you do reflects on you.
- Read With Your Eyes Open. Assess the credibility of information.
- Think Before You Post. Protect your reputation and respect others.
- Connect Safely. Interact safely with others online.
- Keep Yourself Secure. Implement security and avoid scams.
- Abide by the Terms. Act in accord with policies, terms, and laws.
- Stay Out of the Garbage. Avoid objectionable and illegal material.
- Don’t Sell Yourself. Disclose and consume wisely.
- Protect Your Face and Friends. Be savvy and civil when networking.
- Cyberdate Safely. Avoid exploitation and abusive relationships.

Embrace Civility in the Digital Age

Embrace Civility in the Digital Age (a program of Center for Safe and Responsible Internet Use) promotes approaches that will best ensure all young people become cyber savvy and that seek to address youth risk in the digital age in a positive and restorative manner. Web site: http://embracecivility.org E-mail: info@embracecivility.org

© 2011 Embrace Civility in the Digital Age. Permission to reproduce and distribute for non-profit, educational purposes is granted. Embrace Civility in the Digital Age is reliant on sponsorships and donations. If this document is widely distributed, a donation is requested. See our web site for more information.

Nancy Willard’s new book, Cyber Savvy: Embracing Digital Safety and Civility (Corwin Press), and online course, Cyber Savvy: Promoting Students’ Safe and Civil Internet Practice (Knowledge Delivery Systems) extensive insight into effective instructional approaches.