Internet Safety and Responsible Use in a Web 2.0 World

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Use of the Internet
Web sites: http://csriu.org and http://cyber-safe-kids.com
E-mail: nwillard@csriu.org

Shifting from Web 1.0 to Web 2.0

Web 1.0 was largely one-directional – Web as information source.

- Old issue: How do we protect children from seeing inappropriate content?

Web 2.0 is participatory. All users can easily post information online and interact with others. Web 2.0 is also highly mobile. Shifting from desk-top to personal digital devices.

- New issue: How do we prepare young people to safety and responsibly contribute and collaborate in the online world?

Challenges

- Knowing how to effectively participate in the Web 2.0 environment is **essential** for careers, personal life activities, and civic engagement in the 21st Century.

- Many young people are using these new technologies safely and responsibly. Some young people are at risk from others in this environment and some are engaging in inappropriate activities. These are concerns we must address.

- The way in which the Internet has been implemented in most schools has been appropriate for the Web 1.0 environment, but will not be effective in the Web 2.0 environment.

What Is Not Working

Web 1.0 Internet safety approaches are not working.

- Fear-mongering. Prevention research has clearly demonstrated that fear-based approaches are not effective. Young people dismiss Internet fear messages as evidence that adults fear what they do not understand.

- Simplistic rules. Simple guidelines are appropriate for children. Tweens and teens need the knowledge, skills, and values necessary to make good choices online.

- Filtering. Filtering will not prevent accidental access or deter a determined teen. Overreliance on filtering has led to false security and many other concerns.

Not Equally At Risk Online

Young people are not equally at risk online. Youth risk online must be viewed from the perspective of adolescent risk.

- Savvy teens, generally older and with good values, are making good choices online.

- Naïve teens, generally younger, may make mistakes when joining environments with much greater interactivity and the ability to publish. They can become savvy with education and experience.

- Teens who are vulnerable teens and truly “at risk” in the “real world” are at significantly higher risk online. They are more likely to be searching for acceptance from people online and susceptible to manipulation. They are less likely to pay attention to Internet safety messages and more likely to make bad choices. They are less likely to ask for help, even when they really should.

Cyber-Safe Kids, Cyber-Savvy Teens Approach

When children are young they need a safe online environment and simple rules. Parents and schools must be responsible for establishing safe places. As they grow and their activities expand they must know how to independently make good choices online. Parents and educators must remain engaged. Tweens and teens must know what the risks are and how to avoid risky situations, detect if they are at risk, and effectively respond, including when to ask for help. They need to know how to make good choices.

We also must address the concerns of teens who are at higher risk online by educating adults who are likely in the best position to detect and respond to concerns involving higher risk youth online and developing effective teen “bystander strategies.”

Cyber-Secure Schools

To create cyber-secure schools will require: Comprehensive joint planning by safe schools and educational technology. Increased professional and curriculum development. More effective methods for supervision and technical monitoring. Education of students, parents, and staff. Ongoing evaluation.

Policy Issues – What is Needed

- Greater research funding to address youth risk online from the perspective of adolescent risk.

- Coordinated planning to address youth risk online at the state and local level involving state departments of education safe school and educational technology staff, law enforcement, mental health, and consumer protection. Funding to implement these plans.

    - Amend NCLB to require state, district, and school improvement plans to address youth risk online to be accomplished as a joint effort of safe school and educational technology departments. (Elementary and Secondary Education Act of 1965, as amended, Title II, Part D - Enhancing Education Through Technology and Title IV, Part A, Subpart 1. Safe and Drug-Free Schools and Communities).
    - Recognize there will be a need for a waiver for the requirement of implementing programs based on scientific-based research because there is insufficient research-based understanding on youth risk online, research on effectiveness of approaches, and the technologies are rapidly changing. Following the requirements set forth in Section 4115(a)(3) of the SDFSCA can ensure success and accountability.

Policy Issues – What Is Not Needed

- Congressional dictates regarding particular ways in which that states, schools, libraries must address these concerns.

    - Eg. The CIPA mandate for filtering has restricted the development of more effective monitoring and educational approaches to address student Internet use concerns.

- Ear-marked funding for Internet safety curriculum or providers.

    - This approach works against the development of the highest quality programs because funding is based on connections, not quality. States and local education agencies have the best ability to determine quality.