From Safety to Literacy: Digital Citizenship in the 21st Century

How the focus of Internet-safety education has evolved from teaching 'stranger danger' to raising ethical and responsible cyber-citizens.

BY MARSALI HANCOCK, REBECCA RANDALL, AND ALAN SIMPSON

Editor's Note: Last year, the Children's Internet Protection Act (CIPA) was amended to require that E-Rate recipient schools (those receiving discounts for Internet service) provide Internet-safety education to students. Now is the time for all schools, particularly E-Rate schools, to re-evaluate standards and curricula to offer a more comprehensive approach to Internet safety. The iKeepSafe Digital Citizenship C3 Matrix and Augmented Technology Literacy Standards on pages 15–18 will help educators and developers prepare students to become ethical, responsible, and resilient digital cyber-citizens.

In 1950, Congress passed the National Science Foundation Act, which provided for the creation of an alternate communication venue in America. Forty-two years later, in 1992, Congress amended that act to allow commercial traffic to flow through that alternate venue—the Internet backbone. That amendment provided for the modern-day Internet and with it, a new movement in education: Internet safety.

What began as simple safety messages to warn communities about predators and pornography has grown into a vital branch of modern education, covering a host of subtopics within technology literacy, media literacy, safety, and ethics. From that beginning to today's push for integrated standards and curricula—where all disciplines embrace the needs of children online—is the history of Internet-safety education in America. And as connected technologies continue to reach further into our personal lives, we foresee a future in which K–12 educators have proficiency in the emerging area of digital citizenship.

As educators, we can follow the lead of the National Cyber Security Alliance (NCSA) in measuring our success as the NCSA measures its success. We succeed "to the degree that cyber security has become second nature for all computer users … and to raise awareness of cyber security to the level of other cultural messaging that is universally good for citizens—healthy eating, exercise, and safe driving—by teaching skills and judgment to build a national understanding about appropriate online tools and behavior."

The Evolution of Internet-Safety Education

By 1995, with increased Internet access and the proliferation of chat rooms and instant messaging, law enforcement and security experts recognized a growing information gap. The general public did not understand online risks for children. As cyber-crime expanded, crime watchers were the first to identify the fallout.

The Department of Justice responded nationally in 1998 with the creation of Internet Crimes Against Children Task Force units (ICAC), charged with combating the proliferation of child pornography and enticement. Part of the ICAC mission was community education—to reach parents and school children with safety information—and the early messages centered on predators, pornography, and fraud. This marks the beginning of Internet safety as an educational movement in America. Where they could, ICAC officers went into schools, giving presentations to students and faculty about criminal risks for children online.

In 2001, leading security companies and the Department of Homeland Security founded the National Cyber Security Alliance (NCSA) "to empower and support digital citizens to use the Internet securely and safely, protecting themselves and the cyber infrastructure."

As law enforcement focused on crimes against children, education and security experts began looking at Internet safety from a different perspective. They anticipated many of the problems that students would face with the new technology. Davina Pruitt-Mentle, a researcher and policy analyst at Educational Technology Policy Research & Outreach, describes

early efforts in media education: "As we looked more closely and considered all the aspects of using this new technology, we realized that students needed broader training. Informed educators started by talking a lot about plagiarism; then we added copyright infringement as an important element. Later we had a tidal wave of safety messages as the mainstream media broadcast sensational cases about predators. Security as a part of education still is largely out of the loop in training and teaching."

As the Internet became a more dominant element of the media world, the connection grew between media literacy and Internet safety. Media-literacy advocates, recognizing both the educational benefits and potential dangers of media, have promoted the strategy of keeping kids safe by helping them grow smart about media. As the media-literacy movement embraced Internet safety, the messaging moved beyond crime prevention.

Early efforts to add elements of safety and technology literacy to media literacy began in 1998, when the American Association of School Librarians (AASL) and the Association for Educational Communications and Technology published nine information-literacy standards for student learning. Standard eight explains that 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."

In 2000, Pruitt-Mentle assembled the first C3 Framework for educators, detailing how Internet safety should include much more than warnings against predators and pornography. It expands digital literacy to include three areas: cyber-safety, cyber-security, and cyber-ethics (C3). This new and comprehensive way of looking at technology education grew out of her experience working for the Naval Research Lab as well as teaching high school chemistry and physics. "I noticed that everything was technology-based. I tried to integrate technology into teaching chemistry and physics. However, with the ever-growing popularity of the Internet, I soon found that security issues wre of major concern." She first presented the Framework at the 2000 MICCA Conference (Maryland Association for Educators Using Technology, formerly Maryland Instructional Computers Coordinators Association). The following year, the University of Maryland convened the first C3 Conference to prepare educators to teach the essentials of cyber-safety, -security, and -ethics.

From that original framework, Pruitt-Mentle partnered with iKeepSafe and education and technology thought leaders to produce the iKeepSafe Digital Citizenship C3 Matrix (see page 15). The Matrix outlines three levels of competency for students (basic, intermediate, and proficient) within the three comprehensive topics: cyber-safety, cyber-security, and cyber-ethics.

Media and Digital Literacy Today

Current models of technology and media-literacy standards address many of the C3 topics. AASL Standards for the 21st Century Learner relate to safe and ethical behavior, including: "Use information technology responsibly; seek appropriate help when it is needed; practice safe and ethical behaviors in personal electronic communication and interaction." The International Society for Technology in Education also has National Educational Technology Standards (NETS), and the 2007 NETS for Students include Standard Five, Digital Citizenship, which is: "Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior."

In spite of the standards, new research shows that most teachers do not feel equipped to address questions from students on C3 issues. The 2008 Cyber-ethics, Cyber-safety, Cyber-security (C3) Baseline Study, headed by Pruitt-Mentle and sponsored by the National Cyber Security Alliance (NCSA), looked at C3 educational-awareness policies, initiatives, curricula, and practices currently taking place in U.S. public and private K–12 schools. Key findings revealed profound deficiencies in curricula and teacher preparedness. Pruitt-Mentle summarized the findings by saying, "Even in schools and districts where digital safety, security, and ethics education is implemented, only a few, select topics are taught, such as copyright and predator safety, but no one standard covers the broader topics."

Among the other key findings in the Baseline Study:

Safety: Less than 5 percent of educators said that information on responding to identity theft, predators, bullying, etc., is included in the state curriculum. Only 8 percent of educators surveyed said that this information in included in the health/safety curriculum,

Working with At-Risk Youth

Editor's note: To bring the expertise of the public-health community to educators to help them identify and reach out in new ways to at-risk youth online, iKeepSafe works with Dr. Michael Rich, director of Harvard University's Center on Media and Child Health and the director of video intervention/prevention assessment for Children's Hospital Boston. He offers the following observations on at-risk youth in the online world:

As a physician who cares for adolescents, I recognize the importance of providing them with the knowledge and tools to function as healthy, safe individuals and good citizens of their online society, but I also acknowledge that many youth seek sensation, individuation—even rebellion—in both their offline and online worlds. The Internet abounds with opportunities to seek pornography; unsafe sexual encounters; violence; communities that promote self-destructive behaviors such as eating disorders, self-harm, and suicide; and capabilities for hurting others, from cyber-bullying to predation.

The online world presents not only unique risks, but powerful opportunities for reaching out to all youth. A recent research study showed that, while a high proportion of the young people surveyed had portrayed risky sexual or substance-use behaviors on their public social-networking sites, a single advisory e-mail from a self-identified physician resulted in all of those portrayals being removed from public view. As more students, teachers, clinicians, and parents recognize the signs of risk, they will increasingly be able to intervene on behalf of the at-risk child. Finding new ways to reach at-risk youth is the future of intervention and new social media provide a wealth of opportunities for risk prevention and intervention.

and just 20 percent said that media specialists provide this information.

Security Tools: Just over 2 percent of educators surveyed said that information on installing and updating firewalls and antivirus, anti-spyware, and anti-spam software on a computer is included in the state curriculum; only 22 percent of those surveyed said that this is covered by media specialists.

Behavior: Less than 3 percent of educators said that their state curriculum includes information on teaching students how to protect themselves on social-networking sites and chat rooms. Less than 9 percent responded that the health/safety curriculum includes this information, and only 17 percent indicated that students received this information from media specialists.

How well prepared do educators feel they are to inform their students about C3-related topics? According to the study:

- 75 percent of educators are not comfortable discussing cyberbullying.
- 18 percent are prepared to discuss detecting and avoiding malware.
- 31 percent are prepared to discuss digital media copyright laws.
- 21–30 percent of educators are prepared to advise students on cyber-predator and identity-theft topics, dicuss avoiding cyber-crime, talk about social-networking safety, share requirements for safe passwords, give strategies for protecting personal information, and suggest actions students can take should they receive unsolicited e-mails or instant messages.

And how does the educational system inform students about C3 topics? More than half of educators' responses revealed they do not know how their schools inform students about protecting against, identifying, and responding to cyber-crime. Almost 60 percent indicated they do not know how their school informs students on how to identify signs that documents and e-mails contain viruses. And about one-third of the responses stated standards do not adequately address C3 content. Instead, current policies focus on restrictions.

The Digital Citizenship C3 Matrix expands upon the outstanding contribution of previous guidelines and standards to include all aspects of safety, security, and ethics. The Augmented Technology Literacy Standards for Students graph (see page 18) shows how C3 concepts can be integrated into existing standards ((ISTE/NETS•S, AASL Standards for the 21st Century Learner, AASL/AECT Information Literacy Standards for Student Learning, and the 21st Century Framework).

Going Forward

With curricula already packed, digital citizenship requirements may create a new burden for educators. But if we agree with Eleanor Roosevelt and the ancient Greeks that the true purpose of education is to produce citizens, then raising good digital citizens is as essential today in our web-based communities as growing good state citizens was for the Greeks.

The education community must play a vital, pioneering role in digital citizenship. First, we need to offer more flexible, in-depth professional development in cyber-safety, -security, and -ethics for all teachers, not just the technology coordinator or library-media specialist. (The Baseline Study concluded that 24 percent of educators are very dissatisfied with C3 professional development, and only 5 percent are very satisfied.)

"One of the greatest challenges chief technology and information operators face protecting critical school data is educating the educators and employees to understand key security skills and practices," says Linda Sharp, school security expert and project director for the Consortium on School Networking. "It is vital that everyone connecting to the school servers and the Internet recognize how to protect themselves, their students' data, and the infrastructure. School data is only as secure as the users who connect to it." Going forward, all teachers need the opportunity to receive C3 professional development.

Second, schools should consider using the iKeepSafe Digital Citizenship C3 Matrix. Educators currently using the ISTE/NETS Standards, AASL Standards for the 21st Century

Crime Prevention and Media Literacy

There are multiple frameworks for teaching Internet safety to students, the two most prevalent of which are crime prevention and media literacy.

The crime-prevention framework helps raise the visibility of Internet-safety issues and builds awareness among parents and teachers of the potential dangers for kids online. However, there are concerns that this approach will not resonate with kids, who may see the Internet and digital media as new technologies that adults just don't understand. Our warnings to students can sometimes backfire; they can have a "forbidden fruit" effect and make kids even more tempted to do the things we're warning them against. Additionally, the crime-prevention framework by definition focuses on the law-enforcement aspects of Internet use and does not address other issues.

A media-literacy framework seeks to teach Internet safety through Internet smarts, by educating students about how the digital media world works and teaching them about the content they find online (e.g., why it was created, by whom, for which audience, etc.). Students may be more receptive to this framework, which recognizes their interest in digital media and builds their capacity to make smart and safe choices in what they view online and in creating or posting their own online content. Acknowledging that technology and media are advancing at such a rapid pace, the media-literacy framework provides a more comprehensive approach, involving ethics and information literacy. However, there are concerns that a media-literacy approach downplays some of the potential dangers for kids.

Schools should consider how each of these frameworks, or a combination, will work with their students, teachers, and families. Consider the needs of your community and the available resources.

— R.R.

Learners, and AASL/AECT Information Literacy Standards for Student Learning will benefit by referring to the augmented standards sheet to determine how they may incorporate cyber-safety, -security, and -ethics into their lesson plans. All educators—regardless of discipline—can increase their awareness.

Third, based on research by the Berkman Center for Internet & Society and others at Harvard University, we must engage the public-health community for information and ideas on how to reach at-risk youth in their online as well as real-world activities. A bold new partnership, forged between public health and education, will help educators recognize the indicators of trouble and offer intervention, prevention, and bystander awareness to at-risk youth. For professionals trying to reach this segment of students, online social media is a data mine. Troubled teens leave breadcrumbs as to their state of mind and involvement in risky behaviors, such as comments and interests posted on their online profiles. Intervention through electronic means, by online peers or professionals, has proven extremely effective in some instances. *(For more on this, see pages 5 and 27.)*

Raising Wise Digital Citizens

In 1965, John Culkin, S.J., one of the pioneers of media literacy, wrote, "[a]ttainment of (media) literacy involves more than mere warnings about the effects of mass media and more even than constant exposure to the better offerings of these media. This is an issue demanding more than good will alone; it requires understanding."

RESOURCES

American Association of School Librarians (AASL). www.ala.org/ala/mgrps/divs/aasl/index.cfm

Association for Educational Communications and Technology. www.aect.org

Center on Media and Child Health. www.cmch.tv

International Society for Technology in Education: National Educational Technology Standards. www.iste.org/am/template.cfm?section=nets

Pruitt-Mentle, Davina. "2008 National Cyber-safety, Cybersecurity Cyberethics, Baseline Study." National Cyber Security Alliance, October 2008. staysafeonline.mediaroom.com/index.php?s=67&item=44

"Standards for the 21st-Century Learner." American Association of School Librarians, 2007. www.ala.org/ala/mgrps/divs/aasl/guidelinesandstandards/learningstandards/AASL_Learning_Standards_2007.pdf

StaySafeOnline.org: National Cyber Security Alliance. www.staysafeonline.info

The schools and districts that invest in professional development for teachers across all disciplines will see the greatest return in their students' ability to protect themselves and the infrastructure, as they benefit from the positive resources available online. There is no shortcut for rearing a generation of competent and confident Internet users.

The good news is that educators are compulsive teachers. If they have the information, they will share it—even if it doesn't fall under their specialization. This is the future of education for digital citizenship. The best way to train ethical, responsible, and resilient cybercitizens is to have ethical, responsible, and resilient teachers who are comfortable navigating the digital world.

We hope that all educators will feel empowered to meet the needs of the thriving digital citizens of the future.

Marsali Hancock is president of Internet Keep Safe Coalition.

Rebecca Randall is vice president of outreach at Common Sense Media.

Alan Simpson is director of policy for Common Sense Media.

A More Balanced Approach: Beyond Law Enforcement

As law enforcement officers are often the first to identify emerging criminal threats to children, they have played a significant role in informing communities about cyber-crime, such as sexual exploitation, identity theft, and recruitment of gang members. As important as messages from law enforcement are, however, they represent only a small fraction of the skills youth need to thrive as digital citizens today.

Messages that only warn against cyber-crimes do not reflect many of the problems encountered by teens in digital environments. For example, one of the most universal outcomes of a Web-based society likely to affect all teens is the creation of an online reputation that will follow them for the rest of their lives. The posting of compromising content on sites such as Facebook, MySpace, or personal blogs may affect college admissions and future job opportunities.

Trusted educators have the opportunity to help students create an online reputation that is an asset rather than a liability. They can help students understand the potential long-term consequences associated with connected technology and convey the broader ideals of citizenship. Educators empowered with effective messages can help protect the health, safety, and reputation of students online. For this reason, training in cyber-safety, cyber-security, and cyber-ethics needs to be integrated into multiple disciplines of K–12 education.

We must adjust our education to reflect the products that kids use today. Simple messages reiterated by all teachers over the course of K–12 education will have a much greater impact in creating contributing citizens than once-a-year, single-focus presentations from law enforcement. In this environment, every educator teaches tech education. *—M.H.*