Online safety requires ongoing professional learning for staff and continuing education for parents.

By Sandra A. Trach
Laptops. Tablets. Chromebooks. Smartphones. Never have schools had access to tools that offer such wide-ranging potential to impact teaching and learning, but at the same time create such palpable concern about student safety. As schools and districts build their technological infrastructure, they must balance a desire to encourage 21st century learning with a commitment to keep all students safe. The goals of 21st century learning—creativity, critical thinking, communication, and collaboration—cannot be accomplished with a restricted network. Widely used institutional barriers such as filters, firewalls, and policies sometimes result in schools clutching a tool that is not meant to be so tightly grasped.

The good news is that schools are beginning to let go of industrialized teaching models in favor of contemporary, technology-based instruction that incorporates blended, flipped, online, and BYOD (bring your own device) learning experiences. Instructional technology efforts and network management systems should directly support these new modes of instruction, providing the educational and technical support needed to help digital engagement flourish. This type of learning can only be realized with open access to devices and the Internet, ongoing professional learning for staff, and a strong home-school partnership that focuses on digital citizenship to keep students safe.

The Connected Classroom
Students no longer consider schools as the epicenter of knowledge. Instead, today’s learners turn to the Internet to research, communicate, collaborate, curate, create, and share—despite institutional policies and restrictions. The results of Project Tomorrow’s Speak Up 2012 National Research Project stand in stark contrast to the traditional methods that still dominate elementary classrooms today. Results indicate that 75 percent of early learners (kindergarten through grade 2) use computers and mobile devices to play educational games on a regular basis, and 45 percent of students in grades 3-5 use smartphones.

Schools have an obligation to prepare students to skillfully navigate the abundance of information that they consume—in and out of school—and to maximize instructional technology to support 21st century learning. According to the National Council of Teachers of English (NCTE) February 2013 statement on the Definition of 21st Century Literacies, students must be able to “develop proficiency and fluency with the tools of technology,” and “manage, analyze and synthesize multiple streams of simultaneous
information.” While students increasingly learn anywhere and anywhere, constantly advancing their personal drive for knowledge and connections, unfortunately, the type of sophisticated, self-directed, digital engagement described by NCATE is not regularly experienced in our schools. Schools are not changing fast enough to keep up with the pace of students’ thirst for learning through digital means.

It is imperative that schools and parents act quickly to increase their own digital literacy skills, especially as technology—and its impact on learning—continues to quickly unfold. Schools must implement a comprehensive focus on digital citizenship to keep students safe online, with parents as partners in the process.

Educators and parents must remember that the Internet is an endless superhighway of information, and that young children benefit from clear guidelines, as well as teacher and parent support and supervision. Children cannot be “dropped off” unsupervised on the Internet fast lane. The moment students access the Internet, they are no longer only in our classrooms or their homes; they quickly find themselves in an informational stream that poses both learning opportunities and inappropriate content.

While some recommend that teachers and parents start children’s digital use in small, incremental steps, best intentions are often quickly outpaced by children’s innate curiosity and motivation. And because it is nearly impossible to completely prevent children from coming across hazards on the Internet, it is insufficient to simply tell students a list of sites to avoid. Instead, teachers and parents should closely engage with young students as they use the Internet and answer their questions along the way. This allows teachers and parents to capitalize on teachable moments and gain insights into children’s thinking and decision-making.

In order to serve as role models of appropriate usage, principals, teachers, and parents must first be digital learners themselves. Being a digital learner allows educators and parents to assist children firsthand as they explore the Internet.

Safety Guidelines
In his book, Why School?: How Education Must Change When Learning and Information Are Everywhere, author Will Richardson explains that despite increased Internet access, “we aren’t suddenly self-directed, organized, and literate enough to make sense of all the people and information online—or savvy enough to connect and build relationships with others in safe, ethical, and effective ways.” He argues that students need help to develop new literacies to make safe and informed digital choices.

Because schools must lead digital citizenship efforts, principals should provide ongoing professional learning to increase staff capacity with both digital tools and digital literacy. Principals and teachers should also regularly integrate instructional technology to demonstrate its potential for learning. Schoolwide, cross-disciplinary digital literacy lessons will help students internalize digital citizenship messages through multi-modal learning.

Principals should actively partner with parents to foster online safety by hosting informational workshops and sending home digital and print resources in native languages. To reinforce ongoing expectations, schools should post digital citizenship guidelines around the school as public reminders. Some basic tenets include:

**Students Should:**
- Be respectful, kind, and honest;
- Talk to your teacher and parent as soon as you see, feel, or experience something that is not right on the Internet;
- Use strong passwords;
- Make sure teachers and parents have all of your passwords;
- Remember that not everyone is who they say they are on the Internet; and
- Use primary sources.

**Students Should Not:**
- Share personal information online;
- Open unexpected messages or unfamiliar attachments;
- Agree to meet people who approach you online; or
- Plagiarize or cheat.

**Teachers Should:**
- Partner with parents regarding the types of devices and digital curriculum their children will use throughout the school year;
- Review the district’s Acceptable Use Policy with parents and students;
- Have students sign a safety pledge that supports device care and digital citizenship expectations;
- Directly teach students how to take proper care of their devices;
- Pre-assess student knowledge and experience with devices and the Web in order to plan instruction;
- Directly teach specific Web skills and applications that you expect students to know and be able to use;
- Engage students in technology as an authentic means toward learning; and
- Pursue professional learning opportunities to strengthen curricular and digital skills.

**Educators and Parents Should:**
- Become digitally literate;
- Keep computers and devices visible for your attention;
- Have students sign a safety pledge and follow site guidelines, as well as teacher and parent guidelines, for their Internet safety.
- Directly teach students how to take proper care of their devices;
It is imperative that schools and parents act quickly to increase their own digital literacy skills, especially as technology—and its impact on learning—continues to quickly unfold.

Implementing District Policies

Additional measures offer students protection while they are online at school. Schools that accept E-rate funding must comply with the Children’s Internet Protection Act (CIPA). CIPA requires that districts have an Internet safety policy that protects student access to inappropriate content, ensures safety with online communications, and monitors online activities. Protection measures such as Web filtering or monitoring software must be in place. Also, CIPA requires districts to illustrate how they are educating students regarding appropriate online behavior, cyberbullying, and social networking.

Principals should thoroughly read their districts’ Internet safety policy and implement the requirements accordingly. Principals are ultimately responsible for clear policy communication, proper implementation, and consistent monitoring. Specifically, principals should:

- Set limits and guidelines;
- Use system controls for devices and websites;
- Understand social networking and photo sharing; and
- Preview websites in advance.

School-based Strategies

In addition to federal regulation, district- or school-designed Acceptable Use Policies (AUPs) and school-based safety pledges are helpful strategies to offer students clear guidelines for appropriate network use, safe Internet activity, and device care. They can also provide a safety net when Internet filtering and monitoring efforts falter; moreover, they can serve as guideposts for curriculum goals.

When developing or adopting AUPs and safety pledges, keep in mind they should be supportive, rather than restrictive, to instructional technology goals. Key elements of AUPs include:

- A clear statement of the district and/or school’s technology mission(s);
- Who the policy pertains to—students, faculty and staff, administration, parents, volunteers;
- How other district policies may be related;
- Uses of technology that are acceptable and unacceptable;
- Legal responsibilities and implications for unacceptable behavior, including disciplinary action;
- Expectations for devices and account passwords;
- Guidance on social media use;
- District position on privately owned devices that are used in the school;
- District position on school-owned devices that are used outside of school;
- Device responsibility and care, including sharing, loss, damage, theft, and insurance;
- Requirements for student privacy and safety; and
- Expectations for system security.

AUPs and safety pledges are only effective if they are fully and consistently implemented. Communicate AUPs and safety pledges to parents early in the year, and encourage families to develop their own Internet pledges to guide children’s home digital activity.

Bridging Digital Learning and Safety

Educators and parents must accept that digital literacy is an essential 21st century skill. Digital literacy must include instruction on Internet safety, as well as what it means to be a digital citizen. Digital citizens understand how to skillfully—and safely—navigate the breadth and depth of the Internet.

Schools must lead the development of digital citizens by providing ongoing professional learning for staff and continuing education for parents. 

Sandra A. Trach is principal of Estabrook Elementary School in Lexington, Massachusetts.