Staying Safe on the Read-Write Web

Lonely when her parents are at work, Sarah spends a lot of time in chat rooms. One evening, she meets a man who seems to "understand" her. After several weeks of communication, Sarah agrees to meet him in person.

Miguel is devastated by a Web site that personally denigrates him that's been created by an unidentified bully.

Linda is removed from the varsity volleyball team after she puts a picture of herself drinking at a party on her FaceBook site.

The incidents above, modeled after actual events, have librarians, teachers, and parents worried anew about the safety of children and young adults using the Internet. The World Wide Web has rapidly changed from a "read only" resource to one where user input is not just allowed, but encouraged. The development of online tools that allow content to be entered, uploaded, edited, displayed, and made public without having any programming skills has made this "Web 2.0" possible.

And schools are still struggling to determine just how to deal with *Problems 2.0* and *Possibilities 2.0*.

What Is Web 2.0—the Read/Write Web?

These are some of the more popular manifestations of the social Web as of fall 2007:

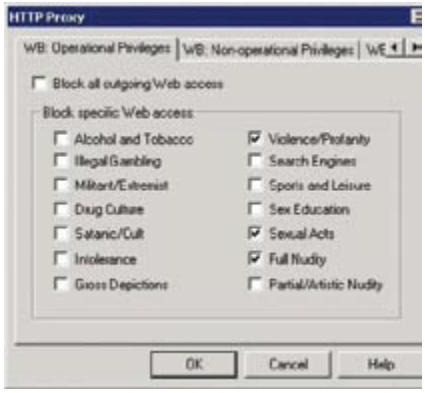
- **Social networking sites** like *MySpace* and *Facebook* are online spaces where users can easily post information about themselves, create lists of friends, and share comments about interests. Fifty-five percent of all online American youths ages 12-17 use online social networking sites.

By Doug Johnson

- **Blogs** (Web logs) are Web sites that are updated on a regular basis, display the content in reverse chronological order (newest entries first), and usually invite reader response. Blogs range in content from personal to political to educational to any conceivable topic.
- **Wikis** are online tools that allow group editing. Individual wikis are simple to set up using free sites like *pbwiki* or *wikispaces*.
- **Social bookmarking** sites like *del.icio.us* allow users to share their Internet bookmarks and create descriptive "tags" to help organize these resources. *Flickr* does the same for photographs, and *YouTube* allows video tagging and sharing.
- **3-D virtual environments** like *Second Life* and *Teen Second Life* allow users to create avatars (pictorial representations of themselves) and explore these worlds; converse with other avatars; participate in virtual economies; create habitats, buildings and objects; look for information; and attend events including classes and presentations.

What are the safety concerns and how valid are they?

Educators have been concerned about the safe and appropriate use of the Internet for as long as it has been available as a resource in schools. The Childhood Internet Protection Act (CIPA) of 2001 requires districts to use a content filtering system to block access to pornography and "sites harmful to minors" if they wish to receive federal funding. This screen shot of a typical filter setting control panel illustrates the kinds of fears adults have about Web 1.0.



The social web, however, is creating a new set of concerns about safe and ethical behaviors of the Internet by students—ones less easily controlled by mechanical solutions such as filters. These include:

- **Protecting children from predators.** Pedophiles using the information gleaned from sites like social networking is arguably the area of greatest concern to parents and educators. According to the National Center for Missing and Exploited Children, "Approximately one in seven youths (10 to 17 years) experience a sexual solicitation or approach while online" and warns parents about the physical abduction of their children.

Other authorities doubt such figures. In its article "Predators & Cyberbullies: Reality Check," Collier and Magid on BlogSafety.com write that in 2005 there were only 100 known cases of child exploitation related to social-networking sites nationwide and that there was "not a single case related to MySpace where someone has been abducted." Nationally recognized Internet safety expert Nancy Willard disputes the figures as incomplete: "This [the figure of 1 in 7 children is propositioned online] is based on 2005 data. The study did not even ask about social networking sites. Most of the inappropriate contacts were in chat rooms, which are far more dangerous than social networking sites. 43% of the solicitations came from other teens and 30% came from folks who self-identified as 18 to 25, so you know...that this also included lots of teens. Only 9% from folks identified as adults over 25. ... But what were the teens doing in these places in the first place[?] 16% of the sexual solicitations came from females and it appears that most of them were under 18. So more female teens [are] soliciting sex online than dirty old men."

- **Protecting children from each other (cyberbullying).** Nancy Willard defines cyberbullying as "sending or posting harmful or cruel text or images using the Internet or other digital communication devices," and she documents instances when such activities have resulted in

severe psychological damage to the victim. According to the Kamaron Institute, cyberbullying incidents have quadrupled in the past five years.

- **Protecting children from themselves (making inappropriate and personal information public).** Larry Magid and Anne Collier in their book *MySpace Unraveled: What It Is and How to Use It Safely* (Peachpit, 2006) argue that the greatest likelihood of children and young adults doing harm to themselves on the social web is by posting pictures and messages that portray themselves in a negative light. This image is then found and viewed by teachers, coaches, relatives, college admission officers, and potential employers. Students don't understand that material once placed on the Internet and made public has the potential of *always* being accessible.

To put it simply, the danger to kids in Web 2.0 comes not from what they may find online, but from what they may put online for others to find.

Steps Schools and Libraries Should Consider to Ensure Student Safety

When the subject of student access to online learning tools is discussed, reactions range from:

> *Until the legal standards and professional practices for filtering, archiving communications in and out of schools, and the liabilities around students posting information about themselves and chatting in a context connected to school are straightened out, it [discussing student use of Web 2.0 tools] is all pretty much a waste of breath.* (Tom Hoffman – Blue Skunk Blog posting)

to:

> *…if something has educational value, is not explicitly illegal and we use due diligence in making kids safe, we ought to give it a try.* (Doug Johnson – Blue Skunk Blog reply)

Here are some actions your school might consider to help keep your students safe and productive on the read/write Web:

1. Examine your AUP.

Our district's current acceptable use policy includes the following language:

> *Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including but not limited to, home addresses, telephone numbers, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identity easily traceable….*

I believe this covers the concerns of both Web 1.0 and Web 2.0. Examine any bullying policies you might have to make sure they cover electronic bullying as well as physical bullying.

2. Block interactive sites.

One knee-jerk reaction has been to block *all* social networking resources—blogs, wikis, YouTube, Flickr, and virtual worlds. American Library Association president Leslie Berger issued a statement highly critical of the nearly unanimous House vote (96%) that passed the Deleting Online Predators bill that would mandate schools block these sites:

> *This unnecessary and overly broad legislation will hinder students' ability to engage in distance learning and block library computer users from accessing a wide array of essential Internet applications including instant messaging, email, wikis and blogs.*

What is problematic about DOPA and school districts' decisions to block blogs, wikis, and chatrooms is that these policies block *formats*, not *contents*. In other words, since a student might place personal information on MySpace, all blogs are blocked. This would be like a school banning all magazines because *Penthouse* is published in magazine format. Formats are content-neutral, but many adults seem to be having a difficult time separating content from format.

Even if social networking sites are effectively blocked in schools, most students will still get access to them. The Pew study, "Social Networking Websites and Teens" (January 2007) found:

> *Teens often use the Internet in several locales, especially home and school. This survey shows that teenagers' use of social network sites relates to the place where he or she uses the Internet most often. Teens who go online most often from home are more likely to report using social network sites than are teens who go online most often from school (42%). Home users are more likely to have profiles posted online (59% compared with 38%) and are more likely to visit social networks once a day or more frequently than are those who go online mostly from school.*

Proxies and mobile networking devices also allow the savvy student to avoid district filters.

To think simple Internet filters will eliminate or even minimize the real risks associated with social networking is a dangerous misconception. It will take educating students about the appropriate use of the Web 2.0 to genuinely protect them.

3. Educate.

Aware schools and parents are using online curricula from organizations like iLearn, BlogSafety, and Responsible Netizen to inform themselves and their children. NetSmartz has created eye-opening videos such as "Tracking Theresa" and "Julie's Journey" that we've shown at faculty meetings. Teachers and library media specialists find these ready-made curricula simple to integrate when teaching Internet safety units.

Our school district, like others, has been actively working to educate communities and parents on issues surrounding Internet safety. We have developed a resource list of Web sites for parents about safe Internet use, have worked with our parent-teacher organizations and community education department to arrange programs about the topic, and have sent home reminders about good computer use in building newsletters.

We have also written materials to help students become aware of the dangers of the interactive Web, including the "ACT NOW" contract (page 51). This warning poster is displayed in our computer labs and libraries.

The Need for the Social Web in Schools—and Children's Lives

Pioneering educators are finding exciting ways to make good use of Web 2.0 resources. Schools and libraries are replacing their newsletters with blogs that can be rapidly updated and allow readers to respond. Teachers are using wikis to facilitate peer-reviewed and collaborative writing projects—including student-created textbooks. Social bookmarking sites are proving to be an efficient means of creating bibliographies and reading lists. Creative teachers are asking students to create Facebook-like profiles for literary characters. (Who *would* be on Juliet Capulet's friends list?) Virtual worlds are allowing students to build historical places and reenact historical events.

And the issues are larger than these resources simply being used to facilitate traditional learning experiences. Henry Jenkins, author of the McArthur report, *Confronting the Challenges of Participatory Culture*, writes:

> *We are using participation as a term that cuts across educational practices, creative processes, community life, and democratic citizenship. Our goals should be to encourage youth to develop the skills, knowledge, ethical frameworks, and self-confidence needed to be full participants in contemporary culture…*

and adds,

> *What a person can accomplish with an outdated machine in a…library with mandatory filtering software and no opportunity for storage or transmission pales in comparison to what person can accomplish with a home computer with unfettered Internet access, high bandwidth, and continuous connectivity…. The school system's inability to close this participation gap has negative consequences for everyone involved.*

Obviously, districts must create a balance between opportunity for student engagement and new teaching methods and the need to protect children. But it is not a simple determination to make.

Vicki Davis on her Cool Cat Blog reflects:

> *…it is not the tools that are inherently good or evil but rather the use of the tools.*
>
> *A hammer can kill someone but it can also build a house.*
>
> *A nail can be driven through a hand but it can also hold the roof over your head.*
>
> *A fist can hit but a fist can also be clasped in your hand in love.*
>
> *We do not outlaw hammers, nails, or fists—we teach people to use them properly.*
>
> *So should we do with blogs, wikis, podcasts, Skype, and any other tool that becomes available for use in the human experience!*

Well said. ■

Doug Johnson is director of Media and Technology at I.S.D. 77 Mankato (Minnesota) Public Schools. He can be reached at doug0077@gmail.com. Doug is the author of *Learning Right from Wrong in the Digital Age: An Ethics Guide for Parents, Teachers, Librarians, and Others Who Care About Computer-Using Young People* (Linworth Publishing, Inc., 2003), *The Indispensable Teacher's Guide to Computer Skills, 2nd Edition* (Linworth Publishing, Inc., 2002) and *The Indispensable Librarian: Surviving (and Thriving) in School Media Centers in the Information Age* (Linworth Publishing, Inc., 1997).

Recommended Web sites about Internet safety:

Center for Safe and Responsible Internet Use
http://csriu.org/

Children's Partnership
http://www.childrenspartnership.org/

ConnectSafely
http://www.connectsafely.org/

CyberBullying information
http://www.cyberbully.org/

CyberSmart
http://cybersmart.org/home/

Family Guide Book
http://www.familyguidebook.com/

Get Net Wise
http://www.getnetwise.org/

iKeepSafe.org
http://ikeepsafe.org/PRC/

McGruff Online Safety for Kids
http://www.mcgruff.org/advice/online_safety.php

MediaWise
http://www.mediafamily.org/resources.shtml

National Center for Missing and Exploited Children
http://www.ncmec.org/

NetLingo: Top 20 Internet Acroynms Every Parent Needs to Know
http://www.netlingo.com/top20teens.cfm

NetSmartz
http://www.netsmartz.org/netparents.htm

Play It Cyber Safe
http://www.playitcybersafe.com/

SafeKids.com
http://www.safekids.com/

SafeTeens.com
http://www.safeteens.com/

Safety Ed International
http://www.safetyed.org/

Wired Safety Website
http://www.wiredsafety.org/parent.html

Of special interest to grades... K-5 6-8 9-12

Dark web websites are often associated with illegal activity â€” but not all of them. Thereâ€™s a chance youâ€™ll find websites run by criminals. Some websites could infect your devices with viruses.Â Accessing content on the deep web is relatively safe. Think about it. You probably check your email and your credit card statements online without worry. But that doesnâ€™t mean that accessing that personal information has no risks. For instance, your accounts on the deep web contain a lot of your personal information that criminals might value.Â Instead, everything stays internal on the Tor network, which provides security and privacy to everyone equally. Worth noting: Dark web website addresses end with .onion instead of the surface webâ€™s .com, .org, or .gov, for example. Whatâ€™s on the dark web? Children need to stay safe on-line and teachers can take practical steps to increase awareness of the dangers. Three simple classroom activities can help h TES | Teaching Resources.Â Cyber Safety. It is important that you read the teacher notes to gain maximum effect for the lesson. The resource is listed in the most effective order to conduct the le TES | Teaching Resources.Â Staying safe on the internet - caught in the web. This resource offers a video which is in two parts and a worksheet to go with it. It aims to address the issues of safety online and in cyberspace. ReadWriteWeb France. 7,018 likes. Rrwf.Â The people who create the hacks on the hit TV show are just as obsessed with getting it right as viewers are. The people who create the hacks on the hit TV show are just as obsessed with getting it right as viewers are. ReadWriteWeb France. 16 July 2016 Â·. Avez-vous Ã©tÃ© attentif au premier Ã©pisode de la saison 2 de Mr. Robot ? https://0x41.no/mr-robot-s02e01-easter-egg/. Mr Robot S02E01 easter egg Torstein July 11, 2016 Malware, Security 9 Comments At the end of S02E01 of Mr Robot, there is a scene where Darlene generate a ransomeware with a modified SET toolkit. My fingers were itching for th Is readwriteweb.com Safe? Trusted site based on user reviews. 4.7. (18 Reviews). Good site. Claim this site. Ask our community. ShareÂ 1. Get alerts about unsafe websites. 2. Block adult content. 3. Stay safe on the go. Share your thoughts Poor. Fair. Average. Good. Excellent. 18 Reviews by the community. Sort by