SCHOOL INTERNET SAFETY

More Than "Block It to Stop It"

Every day, media touches children for good or for evil. Cell phones, computers, and other devices bring everything on the Internet (information, shopping, videos, games, politics, social networking, communication from diverse organizations, and even predators) into a child's intimate world—his pocket, her bedroom, and your classroom. More than half of children and the majority of teens in the developed world regularly access the Internet (2010 studies put the figures at 91 percent of teens in European Union countries, 95 percent in the United States and Japan and 99.5 percent in South Korea).[1] Widespread access to cell phones and Internet cafés worldwide allows many children/teens in the developing world to log onto the Internet. Young people's social networking online[2] creates a variety of risks, such as grooming/stalking by pedophiles and loss of control over personal information. These and other Internet safety risks are defined in Chart 1.

To better understand when and how children and teens encounter these risks, it is helpful to examine their actual Internet use. For example, when young people visit social networking sites such as Facebook, gaming sites, or chat rooms, they interact with "friends," including people they have never met. Chart 2 provides a list of other typical Internet activities along with their associated risks.

How prevalent are risky behaviors among children? According to Dowell, Burgess, and Cavanaugh, most studies about risky Internet behaviors have focused on high school students.[3] In order to gather data on a younger group, their 2009 study involved more than 400 children averaging 12 years of age who were enrolled in two schools (one public, one private) in middle- to upper-middle-class neighborhoods in the northeastern United States. The researchers found that, as with studies of teens, "the majority of youth do not engage in risky Internet behaviors."[4] However, even in an advantaged group such as these children, where one might assume parents or teachers monitor Internet use, a significant minority of children reported engaging in risky behaviors:

- 31 percent of boys and 27 percent of girls **had posted personal information** online.[5]
- 40+ percent of students reported **exposure to inappropriate images.**[6]
- Nearly 30 percent reported **posting rude comments.**[7]

While direct comparison is impossible due to the different ages surveyed, according to Burrow-Sanchez, a 2005 study in the United Kingdom by Livingstone and Bober, which gathered information on 1,511 children between the ages of 9 and 18, reported that 30 percent of participants had met a person online, 46 percent had shared personal information with someone

BY ANNETTE MELGOSA AND RUDY SCOTT

Chart 1. Most Common Internet Safety Risks

Addiction: Excessive time spent on social networking or gaming, which leads users to neglect normal life and relationships.

Cyberbullying: Includes behaviors normally identified as bullying, such as threats and harassment, and publishing untrue or unflattering comments, facts, or photos about other people.*

Grooming/Stalking by Pedophiles or Criminals: Contacts by perverts and criminals online can lead to meetings that result in abduction, exploitation, or death.

Hacking and Viruses: Malicious software (known as malware) is used to steal information (see Identity Theft), interfere with computer functions, or to gain unauthorized access to data. Malware includes spyware (spying on the computer system in the background), adware (advertising that appears without the user's permission), viruses, worms, and Trojans (malware designed to damage computer systems). This can lead to data loss, monetary loss, and/or identity theft.

Identity Theft: Occurs through phishing (e-mails that trick people into revealing sensitive or personal information), downloads from dangerous Websites, or secret installation of software that captures keystrokes.

Illegal or Inappropriate Cyber-Activity: Downloading pirated music, photos, or videos, plagiarism, and hardcore activities like gambling, and child and adult pornography.

Loss of Control Over Personal Photos/Information: Once posted online, personal data, photos/video (sometimes in a compromising situation) are difficult to retract.

Loss of Reputation: Posting information about personal behavior/activities can cause long-term damage to reputation as well as other negative consequences.

* See Susan M. Taylor, "Cyberbullying Penetrates the Walls of the Traditional Classroom," *The Journal of Adventist Education* 73:2 (December 2010/January 2011):37-41.

Chart 2. Online Behavior of Children and Teens

Online Behavior	Description	Commonly Associated Risks
Sharing	Posting photographs, videos, files, and personal information	Cyberbullying, grooming or stalking by pedophiles/criminals, hacking and viruses, identity theft, inappropriate or dangerous ideologies/Websites, loss of control over personal photos/information, damage to reputation.
Online Gaming/Gambling	Playing games hosted by educational or .com sites (.com's use games to sell products), including sites frequented by adults.	Addiction, grooming or stalking by pedophiles/criminals, inappropriate or dangerous ideologies/Websites.
Web Browsing	Searching for homework information, entertainment, or personal interest.	Hacking and viruses; identity theft; illegal or inappropriate cyber-activity; accessing illegal content (photos, text, videos, progaganda, dangerous ideologies, gambling, pornography); inappropriate use of bandwidth (the data channel capacity and speed available for accessing or sharing data), in order to stream movies, etc.
Downloading	Accessing content (photos, videos, music, term papers, presentations) for personal use, to share, or to manipulate.	Hacking and viruses, identity theft, illegal or inappropriate cyber-activity, dangerous ideologies/Websites, plagiarism.

they met online, and 8 percent had had face-to-face meetings with someone they met online.[8]

Internet Safety in School

Today, many schools provide students with Internet access via a computer lab, computers in classrooms, or a laptop or tablet program. Schools must ensure that harmful content is not readily accessible from school-owned or -operated machines. A good way to handle this is to hire a network administrator whose assignment includes keeping harmful content out of the school network, usually through the installation of some form of filter.

Ideally, a properly configured filter will block all content that school policy has defined as inappropriate while allowing access to every site that is deemed acceptable. But filtering technology is not perfect:

Although the ideal would be for parents to monitor their children's Internet use, in homes with multiple computers and high-speed Internet, children often have their own laptop computers and smart phones, making it easy for them to access the Internet without adult supervision.

- *Frequency of filtering error.* Unfortunately, filters tend to be either under- or over-aggressive—failing to block objectionable content (under-filtering) or preventing access to acceptable sites (over-filtering). Time or information lost by users due to over-filtering is a real concern. For example, a science teacher cannot access online science simulations because the school has blocked access to "gaming sites" to prevent students from playing non-educational games online.
- *Resistance to circumvention.* Savvy users may attempt to circumvent filtering technology, engaging the system administrator in a technological arms race and, not unfrequently, "cracking" the system.

While there is insufficient space in this article to discuss the technology solutions available (filters, etc.), if you are a school administrator or board member who must manage Internet filtering for your school, you will find the overview posted at this link: http://circle.adventist.org/files/jae/en/jae2013750355514.pdf to be helpful.

Beyond Blocking/Filtering

Filtering content should be only one aspect of a school's comprehensive Internet education program, which must also include comprehensive policies to (1) protect children from the consequences of inappropriate online behaviors and (2) teach appropriate Internet behavior. However, many schools take the narrow view that filters are *the* safety solution to all of their online problems. Studies show that school personnel often see cyber-safety instruction as unnecessary because the school has locked down its computer systems.[9]

This myopic attitude nearly guarantees that children will fail to learn proper Internet behaviors and will therefore be at risk as soon as they log off of the school network. In some regions of the world, where cybercafés are widely popular, students have access to the Internet without filters or supervision. Although the ideal would be for parents to monitor their children's Internet use, in homes with multiple computers and high-speed Internet, children often have their own laptop computers and smart phones, making it easy for them to access the Internet without adult supervision.

A better way to approach school Internet safety, then, would be for the school to set up a comprehensive Internet safety plan that includes the following:

1. An Internet safety policy, with clear rules, a student contract, and clear consequences for failure to comply (see Section I of http://circle.adventist.org/files/jae/en/jae2013750355514.pdf for more information);
2. Filters (see Sections II and III of http://circle.adventist.org/files/jae/en/jae2013750355514.pdf) for more information);
3. A school-wide Internet safety curriculum.

Basco[10] notes that an inclusive approach to policy development (a committee made up of teachers, parents, administrators, and even students) is more likely to succeed, as it encourages buy-in from all groups affected by the policy. Once a school's Internet safety and use policy is drafted, it should be voted by the school board and implemented throughout the institution.

Internet Safety Education

The need for Internet safety education has been recognized for a number of years.[11] Schools have a responsibility to prepare students for the world that they will face; indeed, the world that they *are* facing. It would seem, then, that understanding how to use the Internet safely is a necessary skill for 21st-century learners.

For the Christian educator, the need to teach about safety stretches beyond the child's career goals to include eternal consequences. Many well-meaning Christian parents and teachers mistakenly believe that strong filters or overbearing rules and prohibitions will protect the child. But nothing could be further from the truth, as this quote from Ellen White shows: "A child may be so trained as to have, like the beast, no will of his own. Even his individuality may be merged in the one who superintends his training; his will, to all intents and purposes, is subject to the will of the teacher. Children who are thus educated will ever be deficient in moral energy and individual responsibility. They have not been taught to move from reason and principle."[12]

In preparing children for a life of service and an eternity with God, we must teach them ethical online behavior (i.e., avoidance of cyberbullying, pornography, and illegal content downloads) within the context of their relationship to God and others. Defining Internet behavior in this way will teach children to ask themselves whether an action exploits and cheapens others and self. Each person can be a conduit of God's love and grace, so not only adults but also children can share God's love with others. Scripture says, "You were bought at a price"[13] and "Those who cleanse themselves . . . will be instruments for special purposes, made holy, useful to the Master and prepared to do any good work."[14]

There is much good to be found on the Internet. Thus, as Christian teachers, it is our privilege to introduce students to uplifting, inspiring, educational Internet resources and to teach them to use the Internet responsibly.

Available Educational Tools

For the school or teacher wishing to implement Internet safety education, a number of initiatives, programs, and educational resources, as well as sample curriculums, are available online and from public school districts. Box 1 includes a number of examples, some of which include an international perspective.

Box 1. Examples of Internet Safety Curriculum Resources on the World Wide Web

360 Degree Safe—http://www.360safe.org.uk/
Developed for southwest England schools, the program provides resources for schools to determine how they are doing when it comes to Internet safety.

Childnet International—http://www.childnet.com
A nonprofit institution with many great resources, including award-winning online projects related to Internet safety.

Tech Parenting Group—http://www.ConnectSafely.org

Internet Keep Safe Coalition—http://www.ikeepsafe.org
A nonprofit, international alliance of educators, law-enforcement agents, policy makers, and technology professionals that provides resources for elementary, high school, and teacher professional development.

Infinite Learning Lab—http://www.learninglab.org
Free Internet safety resources for educators and students.

National Center for Missing & Exploited Children—http://www.netsmartz.org
Free educational materials on the primary or secondary level; includes online games and lesson plans to help integrate Internet safety into a variety of lessons.

National Cyber Security Alliance—http://www.staysafeonline.org
K-12 resources from around the Web in the areas of cybersecurity, cybersafety, and cyberethics.

Think You Know—https://www.thinkuknow.co.uk
Tools for parents and teachers to engage children in conversations about Internet safety.

WiredSafety—http://www.wiredsafety.org/
Cybersafety resources to develop critical-thinking skills.

Another useful tool is the *C3 Framework* (available at http://www.edtechpolicy.org). *C3* was developed to help schools and teachers implement Internet safety standards in a more comprehensive and logical manner. It organizes Internet safety into three distinct yet overlapping areas: cybersecurity, cybersafety, and cyberethics,[15] which may be summarized as follows:

- *Cybersecurity*—how to keep computers safe from malicious software;
- *Cybersafety*—how to safely navigate online while protecting one's personal information and avoiding online predators, financial scams, and other threats.
- *Cyberethics*—how to behave respectfully and ethically (includes topics such as cyberbullying and plagiarism).

C3 has been combined with major information and technology literacy standards, such as those from the American Association of School Librarians (AASL), the Association for Educational Communications and Technology (AECT), and the International Society for Technology in Education (ISTE) in a *C3 Matrix* (available at http://www.ikeepsafe.org/educators/c3matrix/). This valuable resource can serve as the basis for a school Internet Safety curriculum.

How to Teach Cyber Ethics, Safety, and Security

An interesting study done in Greece found that teachers who were more familiar with the Internet were more aware of the dangers, and those who saw value in using Internet applications for educational purposes were more likely to integrate Internet safety lessons into their classroom curriculum.[16] Thus, it would seem that if schools wish to teach Internet safety, they should begin by providing teachers with the tools to successfully integrate technology and Internet safety education in their classrooms. As teachers use technology in their teaching, they will find it easier to develop effective strategies to integrate Internet safety into the curriculum.

Including Internet safety in the curriculum does not necessarily require adding another class. While Internet safety curriculums break down their concepts into learning goals and objectives, in reality, all of these ideas can be taught (indeed, are better taught) when integrated into normal subject lessons. Donovan, Bransford, and Pellegrino point out that "knowledge that is taught in a variety of contexts is more likely to support flexible transfer than knowledge that is taught in a single context."[17] The goal is to help children learn to make wise choices while engaging with the Internet in everyday, practical ways. This will help them transfer the safety skills they learn in class

Chart 3. Examples of Integrated Cybersafety Lessons

Class/Unit	Lesson Content	Description of Lesson
Art—Appreciation of Art Objects	Students visit an art museum online and select a painting, research it online, and prepare an oral or written report.	Discuss copyright/income protection for the artist as a reason why people may not be allowed to download photos of artwork from museum Websites. Also, teach students to evaluate Internet sources—a museum site is more credible than Wikipedia, for example.
Bible—Biblical Characters, Sin, and Redemption	Students identify and explore the experiences of a biblical character who demonstrated bullying tendencies but overcame them through the grace of God (i.e., Saul/Paul).	How people hurt others today with words and actions (example: Compare the early Christians' fear of Saul's threats with how frightening cyberbullying can feel).
Health—Physical Safety and Respect for Others	Students learn that all human beings are made in God's image and that they should respect their bodies and those of others.	How to avoid online solicitation and what to do if the child experiences it; how pornography harms the viewer and the person being exploited.
Social Studies—Learning About Other Regions/Cultures	Using an online forum, students participate with a class in another location to compare lifestyles/cultures.	Teach cyber etiquette and respect when communicating online and how to safely share information and photos. . . .what to share and what not to share.

to their daily Internet activities. They can do this more effectively when the skills are integrated into authentic learning tasks rather than taught as a separate technology class that lacks real-life context. Chart 3 provides a few examples of how Internet safety can be incorporated into the normal curriculum.

Based on a set of Internet safety standards (such as those mentioned earlier in the article), each teacher can assign specific learning goals and objectives to various lessons across various subject areas. If the teacher has already integrated technology into the curriculum, this will make the lessons even more meaningful to students because it transforms the assignments into authentic, Internet-based learning events.

For example, if a teacher normally has students write reports based on Internet research, incorporating a lesson on the rights of authors and simple citation rules will help students to think about plagiarism at the point where they might naturally (intentionally or unintentionally) engage in this behavior. If a teacher has students contact a faraway class via e-mail or chat as part of a social studies lesson, incorporating rules about proper netiquette (how to respectfully address others online) would be a natural part of the lesson. If students use a blog to express their thoughts about various Bible lessons, asking them to read an online testimony of a teen who has been cyberbullied and then to react to it from the perspective of Matthew 5:7: "'Blessed are the merciful, for they shall obtain mercy'" will help students empathize with the victim. When teachers incorporate Internet safety into normal learning activities, this enables students to relate the concepts to actual Internet behavior.

Collaboration With Parents

Another way to teach cyberethics and safety is to enlist the help of parents. Johnson, for example, quotes a 2005 study by Cho and Cheon showing that positive parental interaction (such as sharing Web-browsing activities) decreased the negative content accessed by their children.[18] Since many students have access to the Internet at home, parents should be invited to participate in the school's cyber-education program.[19] As part of the Home and School program, the school can provide a workshop on Internet safety and ethics in the home environment, including topics such as:

- Recommended free filters for home use, and how to set them up.
- Suggested ways of managing Internet use at home (keeping computers out of the child's bedroom, setting time limits; establishing guidelines and consequences for failure to comply).[20]
- Sharing time online (ways to integrate Internet activities into family time).[21]
- Various Internet sites that children might be accessing (social networks such as Facebook, Twitter, etc., movie or music downloading, online gaming communities, etc.) with a discussion of how to teach children to use them safely.

Recommendations

Based on research and experience, we recommend that each school, at every level:

1. Engage stakeholders (parents, school staff and administration, pastors, constituents) in a discussion about Internet safety,

including the Christian philosophy of teaching and learning, defining cybersafety risks and ethics, and exploring possible approaches to ensuring cybersafety at home and school.

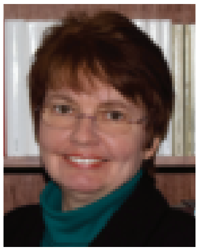
2. Based on that discussion and legal and governmental mandates and guidelines, the school should establish a school Internet-use policy. The policy should include the following elements:

a. A safe network with a professional to administer it, along with clear guidelines and consequences for breaking the rules. (See http://circle.adventist.org/files/jae/en/jae2013750355514.pdf for information about filters and for an example of a student Internet-use contract.)

b. A cybersafety/ethics/security curriculum (including training for teachers on how to integrate technology into their classrooms).

c. A plan for implementing and assessing the policy over time.

A comprehensive school Internet policy such as this will not only protect children while in the school, but will also prepare them to be thoughtful, ethical cyber-citizens in this world and consecrated citizens of the world to come.



Annette Melgosa *works as Instruction Librarian at Walla Walla University in College Place, Washington. In addition to an M.A. in Information and Library Studies, she holds an M.Ed. in Educational Technology and is pursuing doctoral studies in the same field.*

Rudy Scott *owns and operates Pacific Computer Technologies in College Place, Washington. He can often be found fixing computers at nearby Walla Walla Valley Academy or Milton-Stateline Adventist School, and has taught K-12 computing classes and an occasional educational computer technology course for Walla Walla University.*

Technical Information on Filtering Technologies

As an addendum to this article, a large amount of technical information has been compiled and posted online about filtering technologies, along with examples of Internet acceptable-use policies, technical processes, and a chart listing software vendors and the price range of their products, which schools can use when making decisions about how to increase Internet safety for their students and other users. The information can be accessed here: http://circle.adventist.org/files/jae/en/jae2013750355514.pdf.

NOTES AND REFERENCES

[1] Sun Lim, "Internet Safety for Children: A Study of Policy Responses in China, Japan, and South Korea" (Paper presented at the annual meeting of the International Communication Association, Suntec City, Singapore, June 21, 2010), p. 5, EBSCO Communication & Mass Media Complete, AN 59226644; Heidi Seybert, "Internet Use in Households and by Individuals in 2011," in *Eurostat Statistics in Focus* (Luxemburg: European Commission, 2011), No. 66, pp. 2, 3: http://epp.eurostat.ec.eurpa.eu/cache/ITY_OFFPUB/KS-SF-11-066/EN/KS-SF-11-066-EN.PDF. Accessed April 24, 2011; Amanda Lenhart, et al., *Teens, Kindness, and Cruelty on Social Networking Sites* (Washington, D.C.: Pew Research Center's Internet and American Life Project, November 9, 2011): http://pewinternet.org/Reports/2011/Teens-and-social-media/Summary.aspx. Accessed May 7, 2012.

[2] "What Is My Child Doing Online?" (n.d.). https://www.thinkuknow.co.uk/parents/Secondary/What-are-they-doing/. Accessed April 23, 2012.

[3] Elizabeth B. Dowell, Ann W. Burgess, and Deborah J. Cavanaugh, "Clustering of Internet Risk Behaviors in a Middle School Student Population," *Journal of School Health* 79:11 (2009):548.

[4] Ibid., p. 552.

[5] Ibid., p. 549.

[6] Ibid.

[7] Ibid., p. 550.

[8] Jason J. Burrow-Sanchez, et al., "How School Counselors Can Help Prevent Online Victimization," *Journal of Counseling & Development* 89:1 (Winter 2011):3.

[9] Davina Pruitt-Mental, *2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study*. ETPRO-NCSA—Educational Technology, Policy, Research, and Outreach-National Cyber Security Alliance (October 2008), p. 29: http://www.staysafeonline.org/sites/default/files/resource_documents/NationalC3BaselineSurvey_11_14_08_Final_w_forwardpercent2B(3).pdf. Accessed March 2012; "E-Safety Solution From Internet Dangers to School Children," *Manager: British Journal of Administrative Management* 71 (July 2010):11.

[10] Jason Basco, *Acceptable Use Policies in a Web 2.0 & Mobile Era: A Guide for School Districts: Participatory Learning Leadership & Policy—A COSN Leadership Initiative* (Washington, D.C.: Consortium for School Networking, n.d.), p. 3.

[11] Stefan C. Dombrowski, Karen L. Gischlar, and Theo Durst, "Safeguarding Young People From Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet," *Child Abuse Review* 16:3 (2007):153-170; Kevin Butler, "Cybersafety in the Classroom," *District Administration* (June 2010):53, 54; Frank Gallagher, "Hand in Hand: Media Literacy and Internet Safety," *Library Media Connection* 29:4 (January/February 2011):18.

[12] Ellen G. White, *Counsels to Parents, Teachers, and Students* (Mountain View, Calif.: Pacific Press Publ. Assn., 1943), p. 74.

[13] 1 Corinthians 6:20, NIV. Unless otherwise indicated, all Bible quotations in this article are quoted from the New International Version. Scripture quotations credited to NIV are from *The Holy Bible, New International Version.* Copyright © 1973, 1978, 1984, 2011 by Biblica, Inc. Used by permission. All rights reserved worldwide.

[14] 2 Timothy 2:21.

[15] Davina Pruitt-Mentle, *C3 Framework Cyberethics, Cybersafety and Cybersecurity: Promoting Responsible Use* (Maryland: Educational Technology Policy, Research and Outreach, n.d.), p. 2: http://www.edtechpolicy.org. Accessed August 13, 2012.

[16] Panagiotes S. Anastasiades and Elena Vitalaki, "Promoting Internet Safety in Greek Primary Schools: The Teacher's Role," *Educational Technology & Society* 14:2 (2011):77.

[17] John D. Bransford, Ann L. Brown, and Rodney R. Cocking, eds., *How People Learn: Brain, Mind, Experience, and School* (Washington, D.C.: National Academy Press), p. 236.

[18] Genevieve M. Johnson, "Internet Use and Child Development: Validation of the Ecological Techno-Subsystem," *Educational Technology & Society* 13:1 (2010):182.

[19] Jason J. Burrow-Sanchez, et al., "How School Counselors Can Prevent Online Victimization," op. cit., p. 7.

[20] Ibid., pp. 6-8.

[21] Ibid.