



Congress can pass all the laws it wants and civil-liberties groups can challenge those laws, but regardless of what the government does, it's up to parents and kids themselves to assure a safe passage while online.

Larry Magid
GetNetWise.org

A Guide to Online Safety for Kids

The Internet offers opportunities like never before for our children to explore, learn, communicate and entertain. Anyone, however can have a web presence and their intentions are not always beneficial for our children. How do we protect students, children and teens from the potential risks of the Internet, while keeping the information highway open?

Empowering our children to use the Internet safely and responsibly is essential to ensure that school technology plans work. (Teicher, 1999)

What Are The Risks?

• Meeting Someone Online

The most serious problem is a child or teen who is molested or turns up missing as a result of online contact. One behavior attributed to these "meetings" is called "luring." Luring by a person that contacts a child in a chat room or by email can result in a meeting in the real world. Such meetings are highly

dangerous and carry unpredictable outcomes. Because of this threat, it is strongly suggested that chat rooms and emails be supervised by parents.

• Exposure to Inappropriate Online Material

Areas that represent inappropriate online sites are dependent on the child, the family and the community. Such cyber sites often include sexual material or contain violent or hateful content. Children can come upon such sites unwittingly as part of an Internet search. Online predators will sometimes mimic the URL of a popular site.

• Loss of Privacy

Disclosing personal information online such as name, address or phone number can put the child or their family in danger from online predators. COPPA or Children's Online Privacy Protection Act requires websites to obtain parental permission before collecting personal information from children online.

• Cyberbullying

Cyberbullying involves the use of information and communication technologies such as e-

mail, cell phone and pager text messages, instant messaging, defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others.

• Scams and Fraud

Why would a foreign dignitary want to give you money? Did you really win the lottery? The aim of scams and fraud on the Internet is to get you to give out personal information such as access to your bank account or get you to give out your credit card number or get you to render payment in some way. They are commonly sent out as emails but can also be represented online by attractive banners that simulate games. Children are prone to interact with such banners.

Here are some common types of scams:

- Advertising "get rich quick" schemes
- Online auctions, going, going.. uh oh!
- Disaster related scams
- Chain letters (emails)
- Internet Service Providers scam
- Work-at-Home scams
- Health care fraud

• Downloads and Viruses

Computer viruses piggyback on files that you download into your computer. Downloading songs from Internet file sharing sites can bring viruses into your computer. Opening attachments from emails, even emails from friends, can also cause a virus to be downloaded to your computer.



The Law,

COPPA, CIPA & CPPA

The United States Congress has attempted to address the issue of children's online privacy through legislation.

In 1998, congress passed the Children's Online Privacy Protection Act (COPPA).

COPPA specifically protects the online privacy of children under the age of 13. The law requires that websites obtain parental permission in writing before collecting any

More than pornography, I worry about the possibility, however remote, that a child could be harmed by someone he or she encounters online and later meets in person.

-Larry Magid

personal information from children under the age of 13. This law is intended, according to Senator Richard Bryan (D-Nevada), to protect children who participate in online forums.

According to child safety advocate, Lawrence J. Magid, "More than pornography, I worry about the possibility, however remote, that a child could be harmed by someone he or she encounters online and later meets in person. I also worry about online encounters with other kids or adults that could affect a child's self-esteem or threaten a child's privacy... And kids aren't just potential victims of crime. They can also do things online that can hurt others or get in trouble."

Surveys conducted directly after the COPPA enactment, tended to indicate that a large number of websites were still collecting personal information from children under 13. One such survey, conducted in October of 1998, found that of 75 randomly selected sites, 71 collected personal information. Only four attempted to obtain parental permission. (Center for Media Education [CME], 1999).

The government regulatory commission that oversees the Internet is the Federal Trade Commission (FTC). Beginning in 2001, the FTC began reviewing "Safe Harbor" applications.

A "Safe Harbor" website is deemed in compliance with COPPA if they adhere to a strict set of guidelines. More importantly, they include self-regulatory guidelines. The website must submit these guidelines for approval to the FTC before being granted "Safe Harbor" status. The first website to gain "Safe Harbor" status was the [Children's Advertising Review Unit \(CARU\)](#).

In December of 2000, the 106th congress added child safety language to an appropriations bill (funding) in the Labor, Education, and Health and Human Services portion. The language required schools and libraries receiving public funds from federal programs (like the E-rate program and the 1996 Library Services and Technology Act program) to install and use filters on computers to block out obscene online visual depictions of sexually-explicit material, and to monitor the Internet use of students and minors. The provision became known as the Children's Internet Protection Act (CIPA).

Under the same law, there was a provision known as the Neighborhood Children's Internet Protection Act which also required schools and libraries to adopt- after posting notice of and holding at least one local hearing around- Internet safety policies. These policies were to cover information dissemination (including disclosure of personal information) and communication by and with minors using online tools (chat, e-mail, instant messaging, newsgroups, message boards, etc.); unlawful online activities conducted by minors (including hacking); procedures in place to restrict access to objectionable material by minors. It is important to note, however, that the determination of objectionable material is to be made by that individual school, library, or local educational authority.

There is also another set of legal activity regarding the Child Pornography Prevention Act of 1996 (CPPA). This law, in part, made the possession or posting of digital/electronic visual representations of minors engaged in sexual activity illegal (even if the persons in the image were not minors). The constitutionality of the law was challenged in federal appeals court, but upheld in three California U.S. District Courts. The law is now under consideration by the Supreme Court.

Note: Information on CIPA and CPPA obtained through [OMB](#), a non-profit government watch dog organization located in Washington D.C.

What to Do When Problems Arise - Cyber 911

Some cyber-crimes are more serious than others. If any off-line incidents such as abduction, child abuse or death threats occur, contact local law enforcement agencies as soon as possible.

Cyber-crimes such as cyber-stalking, identity theft and child pornography are also serious and need to be reported. These can be reported to online agencies as well as local law enforcement.

WiredSafety.org has a [911 page](#) where the following cyber-crimes can be reported:

[Cyberharassment](#)

[Spam](#)

[phishing](#)

Hacking or Security Intrusions

[Identity Theft](#)

[Scams and Fraud](#)

GetNetWise also has a [page](#) with instructions for reporting cyber-crime. Included are links to Local Law Enforcement, Child Advocacy Groups and Federal Law enforcement.

You have rights. You have a responsibility to protect those rights. Don't be a victim of cyber-crime. Report anything that makes you uncomfortable. Tell your parents first, then make the report if you need to.

Identity theft online can also be reported directly to the [Federal Trade Commission](#).





It's mostly a matter of common sense and knowing a few simple rules.
- Parry Aftab, WiredSafety.org

Safety at School

Statistically, children are safer online at school than at home due to the fact that their online time is supervised and they have limited access to connected computers.

It is important to educate students regarding safe online behavior. Such behaviors include knowing how to avoid risks and knowing good manners (netiquette). Schools need to give the same importance to online safety that is afforded to fire safety or bicycle safety. Safe surfing rules need to be taught as skills, not just given as a list. (see tips on sidebar). In addition to having a curriculum, schools need to have a general policy about Internet use.

In addition, schools need to follow certain guidelines:

Pictures of students posted online should not have names and students should be in groups of four or more.

Follow COPPA guidelines regarding student disclosure of personal information such as name, address email or phone number online.

Provide filtering of online content with appropriate software.

Supervise students while online and set time limits on Internet use.

Most importantly, schools have the responsibility to teach Internet safety skills so that students will learn how to protect themselves whether they are at school, at a friend's house, at home or at the Library.

Types of Internet Filtering Software

List-based software compares the requested URL with a list of sites identified by the manufacturer as having content that violates established criteria. Manufacturers claim 90 to 95 percent success rate. New sites can be added to the list of blocked sites. This type of filtering software is popular for home use. Examples include NetNanny, SurfWatch and CyberPatrol.

Lock-out type filtering permits access only to those sites approved by parents or school administrators. Examples include Kid-Desk and Internet Safe.

Pattern matching filtering software. This type of filtering software looks for certain patterns or terminology found on offensive web pages. No additional monitoring is usually required with this type of software. One example is software called Web Chapperone.

Problems with Web Filtering

Filtering websites is a necessary evil. Schools are required to use filtering software. The management, maintenance and updating of filtering software is up to the school and should be carried out according to district policy and general Internet use plan.

While blocking sites with offensive content, some sites are blocked that would be of use to the student in their guided exploration of cyberspace. Decisions need to be made and teachers and administrators are encouraged to take an active role in Internet filtering decisions.

Tips to Remember

1. Don't Enter Personal Information
Real name, address, phone number and even e-mail address should be kept confidential.

2. Don't Meet Face to Face
Never get together with someone you meet online without checking with your parents.

3. Never Give Out Your Password
Don't give out your password or login information, not even to your best friend.

4. Tell Your Parents
Tell your parents right away if you come across any information that makes you feel uncomfortable.

5. Don't Respond to Mean Messages
Don't respond to any messages or emails that are mean or make you feel uncomfortable in any way. Tell your parents so they can contact the service provider.

6. Set Up Rules
Talk with your parents to set up rules for going online. Decide upon the time of day for you to be online, the length of time and appropriate areas to visit. Don't access other areas or break these rules without your parent's permission.

7. Check With Parents
Check with your parents before downloading or installing software or doing anything that could possibly hurt your computer or jeopardize your family's privacy.

[Adapted from SafeKids.com](http://www.SafeKids.com)



SafeKids.Com

Another consideration is that students need to be made aware that filtering is limiting their choices. Just because a subject does not turn up in their Internet search, does not mean that there are no sites on that subject. Such false conclusions might lead young minds to conclude that there is a justifiable prejudice of content.



Netiquette

Being polite online is also a matter of safety. It is easy to be too abrupt or perhaps not understood when you are not communicating face to face. Sometimes Internet fights can get started. A person online may call you a name IN BIG LETTERS! How should you respond? The answer is that you should tell your parents anytime that someone or something makes you feel uncomfortable online. Here are some basic rules for good online netiquette:

The golden rule is pretty simple: Do unto others as you'd have others do unto you. It applies to online behavior too. Stand up for yourself, but try not to hurt people's feelings. Online, this is called "Remember the Human."

Follow the same standards of behavior that you follow in real life. In real life, most people are fairly law-abiding, either by disposition or because we're afraid of getting caught. In cyberspace, the chances of getting caught sometimes seem slim. And, perhaps because people sometimes forget that there's a human being on the other side of the computer, some people think that a lower standard of ethics or personal behavior is acceptable in cyberspace. Not true!

Be ethical. Always try to do what you think is right. Don't take (download) what is not yours and if you use shareware, pay for it.

Breaking the law is bad netiquette. If you are tempted to do something illegal like downloading copyrighted material, please don't. It is bad netiquette

Respect other people's privacy. Don't read other people's email. If they want to share the contents of their private correspondence, they will show it to you.

Be forgiving of other people's mistakes. Everyone is a beginner when they start. It is polite to overlook minor errors. If you feel the mistake is big enough to warrant a response, state it politely. Remember, you were new once, too.

Safety at Home

Internet safety skills can and should be taught at school, however, the home environment can undo good practices if certain rules are not followed. Just like at school, a policy where rules are discussed works much better than simply handing a list to the child. Here are some suggestions for keeping your children safe at home.

Put the computer in a place such as the family room or den or other room where parents can offer effective supervision. If the computer is placed in a child's room, there is a higher likelihood of non-safe Internet behaviors due to lack of supervision.

Set up guidelines for Internet use. Some of these could include time of day, how much time is to be spent online, what sites can be visited etc. Any change in the guidelines needs to be discussed.

The child should always ask for parental permission before going to a site not previously approved.

It should be made clear to children under the age of 13, that parents must provide consent in writing for collection of personal information by any website. This includes email, name, address or phone number.

Never allow the child to meet a person in the real world that they met online without parental permission.

Inform the child about common scams on the Internet such as false auctions, email scams and chain letters (email).

Ask the child to get parental permission before downloading email attachments, computer applications or songs from the Internet. Such downloads could contain computer viruses.

Install virus protection software on your computer. Spyware and adware can install on your computer automatically when visiting certain websites.

As a parent, you may want to use Internet filtering tools to block offensive websites. See the links below to find software tools to help families protect children from unwanted websites.

Find fun and interesting websites to explore! The Internet is a wonderful place for information, entertainment and fun. The possibilities are limitless. See the links below for some suggested child-safe websites to get you started.

Safety for Different Ages

Computers today are becoming commonplace in the home. When is a child old enough to go on the computer? The following are suggestions for a progressive approach to teaching online Internet safety to different ages.

Ages 2-4 This is a time when children can benefit from "lapware" or exploring the Internet together along with a parent. This insures safety as well as a positive experience.

Ages 4-7 This age can begin to have some independent Internet activity beginning with exploring on a single site. Later, children can explore pre-screened sites and child safe search engines.

Ages 7-10 This age is where children begin to look outside of the family and become more social. Independence can be encouraged with limitations. Filtering software can be introduced at this stage. Also, pre-screening websites and child safe search engines are recommended.

Age 10-12 This is when the pre-teen years begin. This is when children typically begin to use the Internet for school work.

More independence is indicated. Peer influences also come into play. The job of the parents is to help the child manage their independence. In addition to previous measures, it is recommended to set limits on how often and how long the computer can be used.

Age 12-14 At this age children become more interested in online chat. They may also become interested in exploring sexual material online. Make your expectations clear about what is and what is NOT O.K. to explore on this subject. Parents need to develop open communications with children at this age. Some resistance is to be expected. Internet filtering and online monitoring software can be helpful to help parents.

Age 14-17 At this age children are maturing physically, emotionally and intellectually. They are also anxious to experience independence from their parents. This can be challenging for parents, especially since this age statistically engages in risky behaviors, both offline and online. If your teen confides in you about something scary or inappropriate, try to be supportive and work with your teen to help prevent this from happening in the future. And remember that your teen will soon be an adult and needs to know not just how to behave but how to exercise judgment, reaching her own conclusions on how to explore the Net and life in general in a safe and productive manner.

Bibliography

Research Articles

(2002). Cybersmart! internet safety program launched. *Techniques Connecting Education & Careers*, 77(4), 9. This is a short article that announces a collaborative effort by McGraw-Hill, the textbook manufacturer, and CyberSmart, a partner in a national alliance with government and industry, to publish a website to, "...instill young students with a sense of excitement about the Internet and also empower children to use technology effectively and responsibly." Cybersmart offers a free online curriculum for teachers about Internet safety.

[Full Text PDF](#)

Aftab, P. (2004). Online safety at school. *PC Magazine*, 23(13), 58.

Parry Aftab is an Internet privacy and security lawyer. She runs [WiredKids.org](#), the world's largest online safety and help group. In this article she points out that kids are statistically safer when they are online at school vs when they are online at home. The article talks about COPPA (children's online privacy protection act) and the questions schools need to be asking to prevent the spread of online bullies or other online predators. She details what to do should a serious incident occur.

[Full Text PDF](#)

Callister, T., & Burbules, N. C. (2004). Just give it to me straight: a case against filtering the internet. *Phi Delta Kappan*, 85(9), 649-656.

This article presents a case against filtering online content at our schools. Four reasons are cited and support given for each. The first reason is that filtering software does not work as advertised; often blocking legitimate sites along with targeted sites. The second is that filtering is both explicitly and implicitly anti-educational. It sends a message of mistrust to our students. Thirdly, filtering damages the fabric of knowledge because students are unaware that information is available if it has been blocked. The fourth reason given is that there are better solutions, "...if students are spending large amounts of unsupervised time on computers, with little educational purpose in mind, there is a deeper problem at work than any filtering technology can help with."

[Full Text PDF](#)

Coffee, P. (2005). Generation gap. *eWeek*, 22(25), 63.

In this article, Peter Coffee puts forth some important ideas regarding the Internet and child safety. He offers that children are more at risk on the Internet than adults due to their perception of the media as a social environment. He reports on the recent USD Summit on Online Safety held earlier this month (June, 2005) that concluded it is a viable approach to help people learn to recognize dangers that can never be eliminated. Legislating Internet safety is not viewed as being a viable strategy.

[Full Text PDF](#)

Pittman, J. (2000). Making cyberspace safe for children. *Educational Leadership*, 57(6), 68-71.

In this article, Pittman discovers alarming research about the information that is collected from kids as they explore the Internet. In one study 71 out of 75 randomly selected sites, collected information from the user. He discusses protection legislation such as the Children's Online Privacy Protection Act, the use of filtering software and the protection efforts of sites such as [GetNetWise](#) that seek to inform kids about safe online practices. The connection between technology and pedagogy is made evident in this article. Many helpful suggestions are given for parents and teacher's alike to help provide a safe online environment for kids to explore.

[Full Text PDF](#)

Miloradovic, T. (2003). Internet safety, best practices. *Media and Methods*, 40(2), 4.

This article sets forth some ideas about how best to use filtering software in schools. It suggests that an Internet use policy be established in order to take advantage of flexibilities in the software. One such flexibility is filtering content for different age groups. The article also suggests working with the manufacturer to decide which sites should be blocked and which should not.

[Full Text PDF](#)

Teicher, T. (1999). An action plan for smart internet use. *Educational Leadership*, 56(5), 70-75.

This article puts forth the idea that schools need to have just as active a program to promote Internet safety as they do to promote other safety programs such as personal safety, fire safety and bicycle safety. Besides providing details about how to teach Internet safety, the article also contains numerous online resources to URLs covering ethical use, privacy protection and sites for online research. The article warns that, "Communications in the online world have a unique characteristic that can lead to irresponsible behavior: anonymity."

[Full Text PDF](#)

Online Resources

<http://www.wiredkids.org/>

Wired Kids, Inc. is a U.S. charity dedicated to protecting all Internet users, especially children, from cyber-crime and abuse. It operates several programs and Web sites designed to help everyone learn how to protect their privacy and security online and to teach responsible Internet use. This site has a reference to all of the wiredkids, Inc. websites. Including wiredkids.com, wiredkids.org, Tweens and Teens and wiredcops.org among others.

<http://www.surfnetkids.com/kidsafe.htm>

This is Barbara J. Feldman's site for references to Internet safety. Sections include Iggy and Rasper's Tips for Internet Safety and Good Manners, Kid Safety on the Internet, Notes, Advice and Warnings and My Rules for Online Safety, all of which have rules for safe surfing.

<http://www.netbullies.com/pages/1/index.htm>

Cyberbullying is when a student or students target another student with interactive technology harassment techniques. This site explains what schools can do to prevent and plan for cyberbullying. It also gives helpful solutions as well as contact information to report cybercrime.

<http://www.ftc.gov/bcp/conline/edcams/infosecurity/>

This is the official FTC (Federal Trade Commission) site that provides information to kids about safe web surfing. The program's mascot is Dewey, the turtle. There is an interactive quiz for kids to take. The site includes many links to other online resources for Internet safety for kids as well as PDF files for download and printable stickers and posters to promote web safety at your school.

<http://www.internet-safety.org/scripts/content.cgi?template=default&args=guides,introduction>

This site is put together by the Ela Area Public Library, Lake Zurich, Illinois, in conjunction with the North Suburban Library System, and the police departments of Lake Zurich and Hawthorn Woods, who are providing these materials to help educate about safety on the Internet. Funding for this [project](#) was provided by the Illinois State Library, a Division of the Office of the Secretary of State, using federal LSTA funding. The site has sections dealing with crime prevention and awareness, the law governing Internet behavior and transactions, children's awareness and a glossary of terms.

<http://www.cybersmart.org/>

This site offers sections on what students can do to be safe online, what teachers can do and what parents can do. The site offers k-8 curriculum with lessons, standards alignment and scope. There is also a free professional development class that can be taken on online safety through this site. McGraw Hill co-sponsors the site with Cybersmart!

<http://www.getnetwise.org/>

This site's section on kid's safety has components that teach about online safety, tools for families, such as Internet filtering software, web sites for kids and how to report trouble.

<http://www.ftc.gov/ogc/coppa1.htm>

This is the online posting of the 1998 Children's Online Privacy Protection Act.

<http://www.safekids.com/>

[SafeKids.Com](#), [SafeTeens.Com](#) and The Online Safety Project are operated by Larry Magid, a broadcaster and syndicated columnist and author of numerous articles about online safety.

<http://wiredsafety.org/index.html>

Wired safety is a non-profit organization composed of over 9,000 volunteers. It is a cyber-neighborhood that operates as an Internet watch dog service world wide. Parry Aftab, a cyber lawyer and child advocate is featured on this site.

<http://www.internet-safety.org/>

This site is funded by the Illinois State Library, a Division of the Office of the Secretary of State, using federal LSTA funding. The focus is on Internet safety awareness.

Quizzes

http://www.wiredkids.org/ktt_universal/games/javascript/cyberbullying_quiz_1/index.html

A link to wiredkids.org, this site offers an online quiz to inform children about the fundamentals of Internet safety.

http://www.wiredkids.org/ktt_universal/games/javascript/cyberbullying_quiz_1/index.html

This site is an online quiz to help kids understand and know how to respond to cyberbullying. Sponsored by wired safety.

<http://pbskids.org/license/>

This is a site sponsored by PBS. It is an online quiz to get "licensed" to surf the net. The quiz reviews safety rules for surfing the net.

Tools for Families

<http://kids.getnetwise.org/tools/>

This site gives some online tools for finding the right internet filtering software or monitoring software.

Kid Safe Sites

<http://www.internetsuperheroes.org/>

This site also links back to wiredkids.org and offers comic-style storyboard scenarios of situations that might be encountered on the Internet and how to deal with them. It features popular comic book heroes to deliver the content.

<http://kids.getnetwise.org/kidsites/>

This site offers numerous links to kid safe sites. This is a great place to start exploring many fun, entertaining and informative sites.