



Parents' 10 Point Defensive Guide to Children's Safety on the Internet

One Planet Education Network'



Endorsed by The
One Planet Education Network® Seal of Approval
(www.oneplaneteducation.com)

As educators and communications professionals, we recognize parents' need for up-to-date, solid information about online safety. In response to this need, we have collaborated with experts in law, behavioral medicine, education, and Internet communications, to compile new, strategic guide for parents *to aid in making decisions about parental oversight on their children's use of the Internet.* These guidelines have been distilled into a convenient, easily understood format, regardless of prior knowledge. Following the "10 Points" is a sample "Family Contract," a glossary of Internet terms, and a guide to many websites parents should know about.

Traditionally, a parent's role has been to love, educate and keep their children safe from harm. But this may be a unique time in history -- when many young children have *more* knowledge than their parents in certain areas, thanks largely to the Internet.

The World Wide Web is a child's gateway to the outside world, where they can wander freely without ever having to leave the home. In many ways, the impact of this communications breakthrough has been as powerful – and wonderful – as the invention of the printing press or the telephone.

Children are spending ever more time online for education and entertainment, often without their parents' knowledge and guidance. "Remember the advertising campaign, 'It's 10 o'clock – do you know where your children are?'" asks Lisa Ernst, Executive Director of ThinkQuest New York City and an international expert on educational use of the Internet. "Today, a similar campaign might well say, 'It's the Internet age – do you know where your children are?'"

As the Web becomes an increasingly prevalent communications tool, many of today's parents, educators and lawmakers are sailing uncharted waters. With families going online for just about everything, parents in particular have a greater responsibility to become proactive in protecting their children from the dangers of unrestricted Internet use. This ubiquitous, global forum offers very few ways for children to accurately evaluate the consequences of their keystrokes.

Dr. Raun Melmed, a widely respected behavior and development expert and pediatrician, states, "It is the job of parents to protect the kingdom of childhood and set boundaries in all areas. Excessive use of computers, like excessive use of television or video games, should be monitored. Parents must be aware of technology and its capabilities.

"The opportunities to gain solid information and other Internet positives far outweigh the negatives, so it is not prudent to throw the baby out with the bath water. Dr. Melmed, Medical Director of the Melmed Center in Scottsdale, Arizona, continued, "Children and adolescents have no capacity to filter out what may inadvertently turn out to be inappropriate material or data-gathering on certain websites. Children *must* have parental supervision until they are emancipated minors or out of high school."

In response to our request, Charles J. Hynes, the District Attorney of Kings County, NY (Brooklyn) issued this statement:

"The Internet is unquestionably a marvelous and revolutionary tool with the potential to educate our youth in ways never before imagined. At the same time, it can pose serious risks to our children. The safe use of the Internet by children and young adults is a matter of great concern to my office.

"Ensuring Internet safety must be a collaborative effort on a number of levels. Parents must first educate themselves about computers and the Internet in order to learn where potential pitfalls and dangers lie. They must then collaborate with their children to set limits on Internet usage - both with respect to the amount of time their children spend online as well as restrictions regarding certain sites and behaviors. Parents, educators and law enforcement officials must work together to devise the best methods for alerting children to the dangers of the Internet.

"As the chief law enforcement officer of Kings County, I am committed to prosecuting Internet crime with the full force of the law.

"My staff has been trained to carefully review and investigate all complaints of Internet crime that are brought to our attention. In addition, we continue to initiate our own confidential investigations and actively "police" the places where Internet predators hide. I encourage all law enforcement officials across the country to do the same."

10 Point Parents' Defensive Guide

1. Learn as much as you can about the Internet and how the World Wide Web works. There are many books on the subject, or you can take an Adult Education course or ask your PTA or the school's parent coordinator for information.
2. Place the computer in a public area of the home with the screen facing outward – not behind closed doors. (Does this mean restricting your child from having from a computer in the bedroom? The answer is simple: "Yes.")
3. As a family, establish and agree to *written* rules for Internet use that include guidelines for how much time can be spent online and appropriate sites to visit; (see sample "Family Contract" below.)
4. Explain that visiting certain sites can make a computer (and your child) vulnerable by gathering personal information through "spyware."
5. Discuss "netiquette" – polite or appropriate Internet behavior – and what is considered personal information and the dangers of revealing it online, even to close friends. (Be aware that secrets shared online do not stay secret very long.)
6. Explain the risks of meeting people online – through chat rooms, email, --- and the dangers of arranging face-to-face meetings. If you agree to an actual meeting for your child, accompany her/him to a public place.
7. Encourage your child to be critical of all information found online from unfamiliar sources. (Although it's sometimes difficult, learn how and teach your child to recognize scams or phony sites.)
8. Agree not to respond to promotional advertising or free online offers without parental permission and only after thorough investigation as to legitimacy. (They usually ask for personal information and email addresses.)
9. Acknowledge that protecting your child on the Internet is a parental responsibility, not an invasion of the child's privacy.
10. Remember that the positive aspects of the internet far outweigh the negatives. (Information resources, research, communication and project-based learning sites, and, of course, legitimate, non-threatening educational and entertainment sites.)

Family Contract (Family Use Agreement)*

1. We will talk as a family so that we can set up rules for going online.
2. I will agree on the time of day I can be online, the length of time I can be online and appropriate sites for me to visit. I agree to follow the rules and will not access other sites without permission.
3. I will not respond to any messages that make me feel uncomfortable or are bullying. I will tell my parent(s) immediately if that happens.
4. I will not give out any of my or my family's personal information or send pictures without parental permission.
5. I will never give my password to anyone, except my parents.
6. I will assist my parents in learning about the internet and share what I find interesting about the computer.

Child's signature

Parent's signature

* We suggest you post the **Family Contract** in a prominent place in the home, such as on the refrigerator door or next to the computer, as a reminder.

Tech Talk (Glossary)

Alias - an assumed name anyone can adopt online to mask one's true identity. Children often set up a profile using an alias and assume (falsely) that this protects them. They unwittingly disclose personal information that can be directly used to track them.

Blog - This stands for "web log", a very popular online diary children often use to communicate with one another. While potentially a terrific vehicle for writing, it has been abused through the disclosure of personal information and can lead to encouraging unacceptable behavior (bullying or goading bloggers into believing certain behaviors that would not be allowed at home is acceptable among one's peers).

Kids Chat rooms (AOL) - Forums or online places where children can meet online and communicate in real time (live) by typing their conversations and responses to one another. Many who establish an alias and profile to enter these chat rooms are conversing with strangers and are assuming (based on the name of the chat room) that the participants are other children. This may not be the case and could be a forum for predators to meet trusting children.

Cracker - A person who breaks into computer systems, using them without authorization, either maliciously or to just to show off. Today, many people use that definition for the word "hacker".

Cyberspace - This term was first used by novelist William Gibson in his futuristic 1984 novel "Neuromancer" about a world that was dominated by computers and networks. The word now refers to the Internet and the wide range of information and computer networks.

e-pal and groups (public listings vs. unlisted) - What once was known, as a pen pal is not updated to include technology and use of the web. E-pal (or Electronic pal) is someone with whom you communicate online.

Hacker - A hacker can mean an expert programmer who finds special tricks for getting around obstacles and stretching the limits of a system. The term has come to mean a programmer who has gained access to machines or sites without authorization and is often confused with the definition of cracker.

Internet Relay Chat (IRC) - Real-time text conversations similar to that found in chat rooms. Free, but requires knowledge of the recipient's IRC address. Hacker activity is happening here and historically located here.

ISP - Internet Service Provider – refers to the company one pays to get online (such as AOL, AT&T, NetZero, People PC, etc.)

IM - Instant Messaging adding people from chat rooms to your contact list

Netiquette - Abbreviation for Internet etiquette, or accepted guidelines for behavior when online and communicating with others.

Newsgroup (Usenet) - An online discussion group people can respond to messages posted. A group usually has a particular focus, interest, or topic of discussion prompting site visitors to write their views.

ISP Parental Controls - These are controls that parents can activate through software made available by the Internet Service Provider that connects you directly to the Internet. If a family has an Internet account with an ISP used by many members of that family, parents can control access to various sites by settings and passwords for each user.

It is important to note that while these settings might reassure parents that they are protecting their children, these settings are only a first line of defense. Often parental controls do not filter or prevent access to sites parents may wish to block. One should not have a false sense of security thinking that parental controls will provide complete security.

Open Source Software - Refers to software that is created by a development community rather than a single company or vendor. Typically programmed by volunteers from many organizations, the source code of open source software is

free and available to anyone who would like to use it or modify it for their own purposes. (from <http://www.answers.com/open-source&r=67>)

Spyware - This term (as its name suggests) refers to software created to take partial or complete control of a computer without the owner's or user's permission. It secretly monitors or watches how the computer is used with the intention of benefiting someone other than the owner or computer user. (See Wikipedia's definition at: <http://en.wikipedia.org/wiki/Spyware>)

Zombie Computers - A computer that is controlled, through a program planted on it by a hacker that can allow a "cracker" access to information on that computer, and allow that computer to be used to spread viruses or spam email without the owner knowing. Zombie computers can hide the origin of the malicious material being sent.

Zombie Networks - A number of connected (networked) computers that are virus infected and thus can be used to send spam (those unwanted solicitations) making them very hard to stop or trace.

Online Resources for Parents

www.computeruser.com/resources/dictionary/dictionary -- an Internet dictionary
<http://www.computeruser.com/resources/dictionary/dictionary.html>

www.safeteens.com/ - A place for teens and parents to learn how to use the Internet safely.

www.safekids.com/kidsrules.htm

www.ncmec.org: the National Center for Missing and Exploited Children. The NCMEC also maintains a 24-hour multilingual hotline at 1-800-THE-LOST and a website at www.missingkids.com to provide assistance

www.familyinternet.about.com – articles on kids using the internet and parental involvement

www.edu-cyberpg.com - Educational Cyberplayground K-12 Education Reference Directory of Resources

www.WiredSafety.org – a comprehensive online safety and help group

www.wiredkids.org – WireKids is the Official North American Site of UNESCO's Innocence in Danger Program

www.fbi.gov/hq/cid/cac/ncmec.htm -- the website of the FBI unit that deals with missing and exploited children

Chat Rooms Frequented by kids:

www.kidscom.com
www.chatfamily.com
www.chat-avenue.com
www.chatcom.com/
www.headbone.com
www.kidchatters.com
www.yahooligans.yahoo.com/arts_and_entertainment/chat/
www.safekids.com/chatdanger.htm
www.chat-rooms.big.com
www.surfnetkids.com/chat.htm
www.justachat.com/
www.zozanga.com/kids/kid_chat_rooms.htm
www.kidsdomain.com/kids/links/Kid_Chat.html

Blogs parents should be familiar with:

www.xanga.com – An easy on the eye business-like appearance, but a closer look in the blue boxes of featured sites reveals more than meets the eye. Adult content accessible with sexually explicit material.

www.myspace.com – This site has blogs, chat rooms, live video chat, and more. There is a live chat by claims to be by age category. Provocative video clips and images are on the home page. – requires “signup” with information for account to be created. Adult content visible and accessible to site visitors.

www.livejournal.com - Offers audio files that one can post and listen to. Watch out for the audio which can contain adult material.

www.my-diary.org - In the process of moving files – seems to be run by an individual with a link the contact the site owner if there is any problem with any of the diaries. That link, however, is currently down with a “moving files” notice.

www.freeopendiary.com - Free but also requires personal information to create an account. Adult content accessible to site visitors by category.

www.diaryland.com - Don't be fooled by the childlike cartoon graphics appearance of this page. Graphic adult content posted in the form of explicit text and comic book appearance characters. This home page gives the appearance of being the most welcoming and harmless until you open the posted diaries. Parents beware!

Protecting kids in chat rooms

[www.familyinternet.about.com/ cs/internetsafety1/a/aakidschat.htm](http://www.familyinternet.about.com/cs/internetsafety1/a/aakidschat.htm) – A site owned by about.com that features articles on Internet safety by Marcy Zitz. There are links to articles parents can read in the Parenting and Family section.

www.media-awareness.ca/english/parents - A Canadian non-profit organization that self-claims to be “*one of the world’s most comprehensive collections of media education and Internet literacy resources.*”

www.warningsigns.info/chat_rooms_warning_signs.htm - Run by “Parenting With Dignity” by Mac Bledsoe (through son Drew Bledsoe’s Foundation)

www.bewebaware.ca/english/SafeSites.aspx – Canadian bilingual public education program on Internet safety.

Authors:

Patrice Samara, an internationally recognized communications expert and senior business advisor with over twenty-five years experience in the public and private sectors, a multi-Parent’s Choice and Emmy Award-winner was the creator of the Good Housekeeping Children’s Learning Series and Youth and Violence: The Unanswered Questions After Columbine. She was co-author of “Privacy, Security and Identity in a Networked, Data-Driven K-12 Educational Environment” and the “Exploring the Future of Learning Report”.



Neme Alperstein has taught in public schools for 20 years and is currently teaching fifth grade at The Harry Eichler School in New York City. Named NYC Teacher of the Year 2000, NTTI-WNET Thirteen’s Teacher of the Year 2000, and a Bertelsmann Innovative Teacher of the Year 2003, Alperstein has received grants, recognition and awards for her work as a master teacher from ThinkQuest NYC, WNET’s National Teacher Training Institute, NASA’s Student Involvement Program, the Joyce Theater Dance in Education Program, and the Beaumont Foundation.



Prepared in collaboration with:

Charles J. Hynes, Kings County District Attorney (www.brooklynda.org)

ThinkQuest New York City (www.tqnyc.org)

Dr. Raun Melmed, The Melmed Center (www.melmedcenter.com)

Fido Communications (www.fidocommunications.com)

Digiview Entertainment (www.digiviewus.com)

International Faith-Based Foundation (www.iffoundation.org)

Cornerstone Electronics (www.cst1.net)

The Linux Loft (www.linuxloft.com)

Art Circuits (www.artcircuits.com) for Spanish translation

Contact:

Jonathan Slaff

js@jsnyc.com

212.924.0496

© 2006 Patrice Samara and Neme Alperstein

All Rights Reserved

Registered with the Library of Congress