

Do you feel overwhelmed about protecting children from the dangers of the virtual world? We're here to help.

Defending children against online dangers can seem like a daunting task. While there is no silver bullet to keep kids safe online, there are some simple steps you can take to help children enjoy the many benefits of the Internet. The Internet Safety 101™ *Rules 'N Tools*® Booklet is part of the Internet Safety 101™ program, a widely acclaimed teaching series, led by Internet safety expert Donna Rice Hughes, that paints a comprehensive picture of the dangers children encounter online.

The Internet Safety 101™ *Rules 'N Tools*® Booklet covers the essential technical and non-technical safety basics you need to know to become equipped to protect children from pornography, sexual predators, and cyberbullies, as well as how to keep kids safe on social networking sites, gaming and mobile devices.

"If parents don't use safety rules and appropriate tools to keep their kids and families safe, your child is going to receive unwanted content and encounter someone who has ill-intent. If you take those simple basic steps, you maximize the likelihood that your child will be safe and able to use the Internet for all the wonderful benefits it brings."

— Ernie Allen, President & CEO
National Center for Missing and Exploited Children

"You need some rules, you need some tips and you need some tools. They complement one another, one without the other is not the right approach. You have to use them in conjunction with each other and with some common sense."

— Tim Lordan, Executive Director
GetNetWise

"You can give children all the rules that you can possibly think of, but you need parental controls because they can inadvertently come across inappropriate content. Parental controls are a necessity!"

— Holly Hawkins, Director, Policy and Regulatory Division
America Online



Donna Rice Hughes
President, Enough Is Enough
Executive Producer, 101 DVD



"Donna is one of the leaders in the fight against pornography aimed at children on the Internet!"

— Oprah Winfrey

"By implementing *Rules 'N Tools*® on all Internet-enabled devices, parents can better protect their children from dangers online."

—Donna Rice Hughes, President, Enough Is Enough

Internet Safety 101™
***Rules 'N Tools*®**
Booklet

Educate • Equip • Empower

Enough Is Enough
746 Walker Road – Suite 116
Great Falls, VA 22066
1-888-744-0004



NATIONAL SPONSORS:



www.enough.org

www.internetsafety101.org

This package was prepared by Enough Is Enough and funded in part under cooperative agreement numbers 2005-JL-FX-K198, 2007-JL-FX-K006 and 2009-DD-BX-0093 from the Office of Juvenile Justice and Delinquency Prevention (OJJDP), U.S. Department of Justice.



www.enough.org www.internetsafety101.org



Rules 'N Tools[®]

TABLE OF CONTENTS

⊙ Introduction	2
⊙ <i>Rules 'N Tools</i> [®] Internet Safety Guidelines	4
⊙ <i>Rules 'N Tools</i> [®] Checklist	11
⊙ <i>Rules 'N Tools</i> [®] Parent's Pledge	12
⊙ <i>Rules 'N Tools</i> [®] Parent Buddy Check	13
⊙ <i>Rules 'N Tools</i> [®] Youth Pledge	14
⊙ <i>Rules 'N Tools</i> [®] Age-Based Guidelines	16
⊙ <i>Rules 'N Tools</i> [®] Glossary of Terms	21
⊙ <i>Rules 'N Tools</i> [®] Top 50 Internet Acronyms Parents Need to Know	27
⊙ <i>Internet Safety 101</i> SM DVD, Workbook, and <i>Rules 'N Tools</i> [®] Booklet User Guide	28



Rules 'N Tools®

INTRODUCTION

Thank you for joining our efforts to make the Internet safer for children and families! Since 1994, Enough Is Enough (EIE) has been on the frontlines of efforts to protect children online. Year after year, one thing remains constant: parental and adult involvement is the key to protecting kids online! Whether you're a parent, grandparent, guardian, or educator, our goal is to educate, equip, and empower you to protect the children under your care from Internet dangers.

Despite the Internet's many wonderful benefits, a perfect storm has emerged for the online victimization of children because of the intrusive and graphic nature of unregulated pornography, sexual predators easy and anonymous access to kids, law enforcement limitations and challenges, naive kids engaging in risky online behavior, and uninformed, ill-equipped, or overwhelmed parents.

Defending children against these dangers can seem like an overwhelming task. While there is no silver bullet to keep kids safe in the virtual space, the good news is that you don't need a Ph.D. in Internet technology to be a great cyber-parent. However, you do need to make a commitment to become familiar with the technology your children use and to stay current with Internet safety issues.

Over the years we have seen that, although the content and the capabilities of the Internet have evolved, the basics you need to know to keep kids safe in this ever-evolving digital world continue to hold true. Although kids are now at risk of encountering inappropriate content and dangerous people across multiple Internet platforms, the basic modus operandi utilized online by the pornography industry and sexual predators have not significantly changed. Even more promising: the basics of Internet safety have not changed significantly, either. It's upon these fundamental Internet safety principles—basic safety rules and software tools (*Rules 'N Tools*®)—that we have built our national reputation for effective Internet safety education.

To use a sports analogy: the best coaches often teach their teams the basic plays of the game and train them to execute those plays well. In this *Rules 'N Tools*® Booklet, we hope to teach you the fundamentals of Internet Safety 101™ *Rules 'N Tools*® and equip you to implement these basic measures to help you to become an empowered protector of the children entrusted under your care.

We strongly encourage you to use this booklet in combination with the full Internet Safety 101™ program curriculum, which combines the most critical Internet safety information with testimony, advice, and information from the leading experts, clinicians, law enforcement, parents, teens, industry leaders a survivor of Internet predation and even a sexual predator in a compelling, all-inclusive DVD teaching series and accompanying workbook. To find out more about this program, visit us at www.InternetSafet101.org or call us at 888-744-0004.

Now let's get started!

For the Sake of the Children,



Donna Rice Hughes

EIE President and Chairman





RULES 'N TOOLS®

Internet Safety Guidelines for Parents, Educators, and Other Caring Adults

Implement *both* safety rules and software tools to protect children online. Focus on the positives of Internet use while teaching children about the dangers and how to make wise choices online.

“RULES”

NON-TECHNICAL MEASURES

As technology continues to evolve, it is easy to feel left behind. Follow these non-technical measures to help you become a cyber-savvy, virtual parent.

! **Establish an ongoing dialogue and keep lines of communication**

open: Spend time online alongside your children and create an atmosphere of trust. Encourage your children to make good choices and temper your reactions when they run into dangers.

Teens whose parents have talked to them “a lot” about online safety are less likely to consider meeting face-to-face with someone they met on the Internet (12% vs. 20%).ⁱ

! **Supervise use of all Internet-enabled devices:** Keep your child’s computer in an open area of your home. Monitor other points of Internet access including your child’s cell phone, portable music device, gaming device, and PDA.

ⁱ Cox Communications Teen Internet Safety Survey, Wave II—in Partnership with the National Center for Missing & Exploited Children, March 2007. <http://www.cox.com/TakeCharge/includes/docs/survey_results_2007.ppt#271,1,Slide 1>



- ! Know your child's online activities and friends:** Be familiar with each of your children's passwords, screen names, and all account information, and have them provide the identities of every person on their buddy list or anyone they have "friended" on social networking or gaming sites. Caution your children to only communicate online with people they know in-person and who have been approved by you. Remind your children that the people they meet online may not be who they say they are.

Almost 1 in 8 teens discovered that someone they were communicating with online was an adult pretending to be much younger.ⁱⁱ

- ! Regularly check the online communities your children use, such as social networking and gaming sites, to see what information they are posting:** Make sure you, as the parent, are added to your child's "friend list," because if their profiles are set to private (as they should be!), you will not be able to view any of their information. If you are unsure whether your child has a profile, conduct a simple online search through the site or by typing their name into a search engine (e.g., Google). Be aware of not only what your children are posting, but what other kids are posting about your children. Before allowing children to use social networking sites, EIE encourages parents to familiarize themselves with the content on the site and thoroughly review the safety practices and privacy tools available through that social networking site.

- ! Supervise the photos and videos your kids post and send online and through their mobile device:** Photos and videos can be uploaded instantly to sites like YouTube and Facebook from any platform with Internet access including your child's cell phone, webcam, PDA, and gaming device. These images may make your child vulnerable to online predators, cyberbullies, and strangers, or lead to damaged reputations. Check with your child's school to ensure that any projects, art, or photos placed on the school website are only accessible by password (or through the school's intranet) and do not contain any personally identifiable information. Younger children should not post, text or send photos or videos.

4% of all youth Internet users in 2005 said online solicitors asked them for nude or sexually explicit photographs of themselves.ⁱⁱⁱ

ⁱⁱ Internet Safety: Realistic Strategies & Messages for Kids Taking More and More Risks Online. Polly Klaas Foundation, 2006.

ⁱⁱⁱ Wolak, Janis, Kimberly Mitchell, and David Finkelhor. Online Victimization of Youth: Five Years Later. Alexandria, Virginia: National Center for Missing & Exploited Children, 2006.



! Discourage the use of webcams and mobile video devices: Most computers, cell phones and other mobile devices now come with built-in webcam and video devices, but videos and webcams should only be used under close parental supervision or not at all. Videos should only be sent to trusted friends and family. Never allow a webcam or mobile video device to be used by your child in his or her bedroom or other private areas.

! Teach your children how to protect personal information posted online and to follow the same rules with respect to the personal information of others: Remind your children to **think before they post: there are no take-backs online.** Nothing is truly private on the Internet; any and all information sent or posted online is public or can be made public.

Caution your children about posting:

PERSONAL OR CONTACT INFORMATION: Your child's full name, address, phone number, passwords, and financial information should only be provided on a secure site and under parental supervision.

INTIMATE PERSONAL INFORMATION: Private, personal, and sensitive information (such as a teen's journal) should not be posted and should only be shared in private e-mails with a trusted personal friend.^{iv}

REPUTATION-DAMAGING INFORMATION OR IMAGES: Inappropriate pictures (i.e., content that is explicit, suggestive, illegal, etc.), should never be posted or sent.^v

EVENT INFORMATION: Teach children to use caution when posting information about parties, events, or activities where someone could track them down.

Teens whose parents have talked to them "a lot" about Internet safety are more concerned about the risks of sharing personal information online. For instance, 65% of teens whose parents have not talked to them about online safety post information about where they live compared to 48% of teens with more involved parents.^{vi}

^{iv} Willard, Nancy E. *Cyber-Safe Kids, Cyber-Savvy Teens.* Jossey-Bass, 2007.

^v Ibid.

^{vi} Cox Communications Teen Internet Safety Survey.

! Be sure your children use privacy settings: Privacy settings limit who can view your teen's profiles. On most social networking and gaming websites, your teen can change his or her privacy setting by clicking on "account settings." Ask your teens to show you the account



settings or, if you have access to your teen's account, you can check their settings for yourself. Remember that no one can detect a disguised predator, and even using these settings does not always achieve true privacy: all of your child's friends have access to and could distribute any material included on their profile.

47% of teens have an Internet profile that is public and viewable by anyone.^{vii}

! Instruct your children to avoid meeting face-to-face with someone they only know online or through their mobile device: Online and mobile 'friends' may not be who they say they are. Children should be advised to come to you if anyone makes them feel scared, uncomfortable, confused, asks for any personal or personally identifiable information, or suggests meeting them.

16% of teens say they've considered meeting face-to-face with someone they've talked to only online, and 8% of teens say they have actually met in-person with someone from the Internet.^{viii}

! Teach your children how to respond to cyberbullies: Children do not have to accept any online activity meant to intimidate, threaten, tease, or harm them or anyone else. Watch out for warning signs, including reluctance to go to school and reluctance to use the Internet; be aware of a change in your child's behavior and mood. Report any offensive or dangerous e-mail, chat, or other communications to local law enforcement. Do not delete the evidence. Remind your child of the Golden Rule: "Do unto others as you would have them do unto you."

Overall, 19% of teens report they have been harassed or bullied online, and the incidence of online harassment is higher (23%) among 16- and 17-year-olds. Girls are more likely to be harassed or bullied than boys (21% vs. 17%).^{ix}

! Establish an agreement with your children about Internet use at home and outside of the home (see *Rules 'N Tools*® Youth Pledge): Remind them that rules for good behavior don't change just because they're on a computer. Post the agreement near the computer. Be willing to sign a parent pledge as well.

^{vii} Willard, Nancy E. *Cyber-Safe Kids, Cyber-Savvy Teens*. Jossey-Bass, 2007.

^{viii} Cox Communications Teen Internet Safety Survey.


^{ix} *Ibid.*



“TOOLS”


TECHNICAL MEASURES

In addition to safety rules, protecting kids online requires the use of software tools, better known as parental controls. Parental control software helps prevent objectionable content and dangerous people from gaining access to your child. A comprehensive suite of parental control tools should include customizable filters, monitoring software, time-managing controls, and Instant Messaging (IM) and chat controls. Parental controls should be utilized on all Internet-enabled devices (desktops, laptops, and gaming, mobile, and music devices). However, these resources are not a substitute for parental supervision.

 **Set age-appropriate filters:** Filters block categories of inappropriate websites a child can view, such as sites containing pornography, violence, gambling, and illegal drug information. Settings are password-protected. Remember that *no filter is a substitute for parental supervision*, and filters may not stop a determined child from bypassing them and accessing unsuitable content. Also, set filters to block access to peer-to-peer (P2P) networks, which allow users to connect directly to each others' computers to retrieve and swap files, without a server, and which contain tremendous amounts of pornography and child pornography.

7 out of 10 Internet users ages 8 to 18 were exposed to unwanted sexual material and more than three-quarters of unwanted exposure to pornography (79%) happened at home.^x

^x *Generation M: Media in the Lives of 8–18 Year-olds*. Henry J. Kaiser Family Foundation. 17 Nov. 2006. Wolak, Janis, Kimberly Mitchell, and David Finkelhor. *Online Victimization of Youth: Five Years Later*. Alexandria, Virginia: National Center for Missing & Exploited Children, 2006.

 **Consider using monitoring software, especially if you sense your child is at risk:** Monitoring software, or keystroke capture devices, can provide a full and complete record of where your child goes online, monitor outgoing and incoming communications, and identify a child's online buddies. More robust monitoring tools let parents see each website their children visit, view every e-mail or instant message they send and receive, and can even record every word they type. Many monitoring tools can send parents a periodic report summarizing their child's Internet usage and communications. These programs empower parents



and guardians to set online boundaries for their children. Parents should tell their children that monitoring is being used unless the parent suspects their child is involved in risky behavior, in which case it may be better to go stealth.

80% of sexual predators are explicit about their sexual intentions. The offenders lure teens after weeks of online conversations, playing on common teen vulnerabilities, such as their desires for romance, adventure, sexual information, and understanding. In 73% of these crimes, the youth meet the offender on multiple occasions for sexual encounters.^{xi}

Periodically check your child's online activity by viewing your browser's history: Watch out for any sites that sound inappropriate (although not every inappropriate site has an inappropriate name!). If you notice the history has been cleared or deleted, have a discussion with your child about the sites he or she visited. Be aware that your child may selectively delete files from the history list. If you are concerned about your child's online activity, you may want to install monitoring software.

65% of all parents and 64% of all teens say that teens do things online that they wouldn't want their parents to know about.^{xii}

Set time limits: Excessive time online, especially at night, may indicate a problem. Remind your child that Internet use is a privilege, not a right. If necessary, utilize time-limiting software tools, which allow parents to manage the amount of time and times of day their children are allowed online.

Disallow access to chat rooms and only allow live audio chat with extreme caution: Chat rooms are the playground of today's sexual predator; they allow immediate, direct communications between participants. Many geared toward adolescents are known for explicit sexual talk and obscene language, fostering an atmosphere which may attract online child molesters.^{xiii} Chat rooms also allow users to communicate via webcam and audio chat.

Many gaming programs also come equipped with live audio chat capabilities through which individuals can alter the sound of their voice. Only mature teens should be allowed to use live audio chat. Remind your child to only interact with individuals they know offline. It's impossible for a parent, child, chat room monitor, or any technology tool to recognize a disguised, anonymous predator.

^{xi}Finkelhor, David, Kimberly Mitchell, and Janis Wolak. National Juvenile Online Victimization Study. National Center for Missing & Exploited Children, 2007.

^{xii}Lenhart, Amanda. Family, Friends & Community: Protecting Teens Online. Pew Internet & American Life Project, 2005.

^{xiii}Subrahmanyam, Kaveri, David Smahel, and Patricia Greenfield. "Connecting developmental constructions to the Internet: Identity presentation and sexual exploration in online teen chat rooms." Developmental Psychology 42.3 (2006) 395-406.



Most sexual solicitation incidents (79%) happened on home computers, beginning with personal questions about the teen's physical appearance, sexual experience, and with propositions for "cybersex."^{xiv}

37% of sexual solicitation incidents happen while youth are in chat rooms, and many occur in live chat or instant-message sessions.^{xv}

- Limit your child's Instant Messaging (IM) contacts to a parent-approved buddy list:** If you decide to allow your child to use IM, block all communications from anyone not on the child's pre-approved contact list. Robust parental control software will prevent your child from adding anyone to their buddy list unless you have approved the addition. However, since some kids are able to bypass parental controls, regularly check their buddy list to ensure that it has not been altered. Be aware that many online communities, such as social networking and gaming sites, now have IM and chat features, and not all parental control software provides coverage over these new chat platforms.
- Use safe search engines:** Although search engines enable your kids to find fun websites and educational information, they can also be an efficient gateway to pornography and other objectionable content. Major search engines have addressed this need by creating child-safe zones. Some give the option of parental controls or safe searches. Consult the information on your ISP's and search engine provider's settings page to make sure that the safe search option is on.
- Set up the family's cyber-security protections:** In addition to setting up parental controls, regularly update the operating system and install a firewall and up-to-date anti-virus and anti-spyware software. The instant a computer is connected to the Internet or an "always on" broadband connection, hackers and thieves can attempt to gain access to the family's financial and personal information. By securing your computer, you can help protect against these Internet intruders and the malicious programs that can infiltrate your computer.

^{xiv}Wolak, Janis, Kimberly Mitchell, and David Finkelhor, 2006.

^{xv}Ibid.

^{xvi}National Campaign to Prevent Teenage and Unplanned Pregnancy and CosmoGirl.com, 2008.

Report any content or activity that you suspect as illegal or criminal to local law enforcement and to the National Center for Missing & Exploited Children at www.cybertipline.com or at 1-800-843-5678.



RULES 'N TOOLS® CHECKLIST FOR PARENTS, EDUCATORS, AND OTHER CARING ADULTS

Implement *both* safety rules and software tools to protect children online. Focus on the positives of Internet use while teaching children about the dangers and how to make wise choices online.

“Rules”

- Establish an ongoing dialogue and keep lines of communication open.
- Supervise use of all Internet-enabled devices.
- Know your child’s online activities and friends.
- Regularly check the online communities your children use, such as social networking and gaming sites, to see what information they are posting.
- Supervise the photos and videos your kids post and send online.
- Discourage the use of webcams and mobile video devices.
- Teach your children how to protect personal information posted online and to follow the same rules with respect to the personal information of others.
- Be sure your children use privacy settings.
- Instruct your children to avoid meeting face-to-face with someone they only know online or through their mobile device.
- Teach your children how to respond to cyberbullies.
- Establish an agreement with your children about Internet use at home and outside of the home (see *Rules 'N Tools*® Youth Pledge).

“Tools”

- Set age-appropriate filters.
- Consider using monitoring software, especially if you sense your child is at risk.
- Periodically check your child’s online activity by viewing your browser’s history.
- Set time limits and consider using time-limiting software.
- Disallow access to chat rooms and only allow live audio chat with extreme caution.
- Limit your child’s instant messaging (IM) contacts to a parent-approved buddy list.
- Use safe search engines.
- Set up the family’s cyber-security protections.
- Utilize parental controls on your child’s mobile phone and other mobile devices.

Parental controls should be utilized on all Internet-enabled devices (desktops, laptops; and gaming, mobile, and music devices). However, these resources are not a substitute for parental supervision.

Report any content or activity that you suspect as illegal or criminal to local law enforcement and to the National Center for Missing & Exploited Children at www.cybertipline.com or at 1-800-843-5678.



Rules 'N Tools®

PARENT'S PLEDGE

I pledge my commitment to implement *Rules 'N Tools®* on all Internet-enabled devices used by my children within the next _____ days.

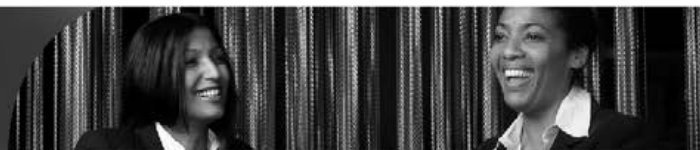
I understand that these protective measures will help prevent objectionable content and dangerous people from gaining access to my children. Being proactive with online safety is an act of love that will help keep my children safe.

Parent/Guardian Signature

Parent/Guardian Signature

Date

Date



Rules 'N Tools®

PARENT BUDDY CHECK

The intent of the Parent Buddy Check program is to empower parents to help ensure that *Rules 'N Tools*® are implemented across all Internet-enabled devices used by their children. To provide an added safety net of support, Enough Is Enough (EIE) encourages every parent to invite another parent or a friend to be their 'Parent Buddy.' *Parents are the first line of defense!*

There are two simple steps to get the Parent Buddy Check program started:

Step 1:

Ask a buddy—a relative, friend, or a co-worker—to support your commitment to protect your children online as represented by your *Rules 'N Tools*® Parent's Pledge.

Buddy Signature

Date

E-mail Address

Step 2:

To promote greater awareness throughout your community, talk regularly with your 'Parent Buddy' and with your friends about the importance of Internet Safety, and be sure to check EIE's website at www.enough.org for the latest tools and resources to protect your family on the Internet.

Together we can make a difference for the sake of the children!



Rules 'N Tools®

YOUTH PLEDGE

I have spoken with my parent/guardian about the following and am aware that:

- Nothing is truly private, and there are “no take-backs” online and through my mobile device.
- Some people online may try to befriend me who want to harm me.
- It is not my fault if I see something bad accidentally.
- Private family matters should not be discussed online or via text. Instead, I should talk about them with a parent or other trusted adult.
- My parents may supervise my time online and may use a filtering and/or monitoring service. This is because they are concerned about my safety.
- Internet use and mobile access is a privilege, not a right. I will follow the guidelines of my *Rules 'N Tools®* Youth Pledge whenever I have access to the Internet, both in and out of my home or through my mobile device.

I agree to:

- Talk with my parents to learn the rules for using the Internet, including where I can go, what I can do, when I can go online, and how long I can be online (_____ minutes or _____ hours).
- Always tell my parents immediately if I see or receive anything on the Internet, my phone or other mobile device that makes me feel uncomfortable or threatened, including e-mail messages, websites, images, chats, or even anything in the regular mail from Internet friends.
- Protect my personal information, such as my home address, telephone number, my parents' names, work addresses or telephone numbers, credit card numbers, or the name and location of my school or any club or team. I will talk to my parents before giving out this information. I will keep this rule when I am communicating via chat rooms, instant message (IM), e-mail, websites, online games, text messaging, or social networking sites, and when entering contests and registering for online clubs.
- Check with my parents before posting or sending pictures or videos of myself, other family members, or other people through the Internet, text or regular mail.
- Never give out my Internet passwords to anyone (even my best friends) other than my parents.
- Treat others online as I would have them treat me. I will never send threatening or mean messages, nor will I respond to any such messages that are sent to me. I will not do anything online that could hurt or anger others or do anything that is against the law.

RULES 'N TOOLS®

- Never download, install, or copy any copyright information from the Internet without proper permission from the site and my parents.
- Never do anything on the Internet or on my cell phone or other mobile device that costs money without first asking permission from my parents.
- Only fill out any online forms or questionnaires with the permission of my parents.
- Never open or accept e-mails, enclosures, links, URLs, texts, videos or pictures or other information from people I do not know.
- Never tell anyone online where I will be or what I will be doing without permission from my parents.
- Never enter a chat room unless given prior permission from my parents.
- Avoid in-person meetings with anyone I met or befriended online or through my mobile device without parental permission and being accompanied by a parent. I know that not everyone I meet online is who they say they are, and I cannot detect a disguised predator.
- Follow my family's Internet safety guidelines when accessing the Internet through an Internet-enabled device, while at a friend's house, and also when at school.
- Only instant message (IM) people on my buddy list who have been previously approved by my parents.
- Log off or turn off my computer if I come across something bad online. I will then tell my parents what happened as soon as possible.
- Make my parents aware of **all** of my Internet login, chat names, gamertags, and social networking profile names listed below:

Youth's Signature

Parent's Signature

Date

Date

**Parents may use this pledge for their children, tailor this pledge to meet the specific needs of their family, or work with their children to create a youth pledge together!*

Rules 'N Tools®

AGE-BASED GUIDELINES

Remember to use Enough Is Enough's Internet Safety *Rules 'N Tools*® to protect your kids at every age!

Key principles for all age groups include to:

- ⊙ Keep lines of communication open.
- ⊙ Create a list of Internet rules with your kids (see *Rules 'N Tools*® Youth Pledge).
- ⊙ Set parental controls at the age-appropriate levels and use **filtering** and **monitoring** tools as a complement—not a replacement—for parental supervision.
- ⊙ Supervise all Internet-enabled devices and keep computers in a public area of the house.
- ⊙ Talk to your kids about **healthy sexuality** in the event they come across sexually explicit, online pornography at home, school, a friend's house, or the library.
- ⊙ Encourage your kids to come to you if they encounter anything online that makes them feel uncomfortable or threatened. (Stay calm and don't blame the child; otherwise, they won't turn to you for help when they need it.)
- ⊙ Teach them not to interact with people they don't know offline because an online predator can easily disguise him/herself.
- ⊙ Check the history file on your computer to see which sites your child has accessed.



TWO- TO FOUR-YEAR-OLDS

KIDS AT THIS AGE:

- ⊙ Will accept media content at face value
- ⊙ Don't have the critical thinking skills to be online alone
- ⊙ May be frightened by media images, both real and fictional
- ⊙ Risk moving from appropriate to inappropriate sites through hyperlinks

GUIDELINES:

- ⊙ Always sit with your child at the computer (EIE recommends that children at this age not be exposed to the Internet).
- ⊙ Parents can begin teaching basic computer skills by introducing age-appropriate games and educational programs.

FIVE- TO SEVEN-YEAR-OLDS

KIDS AT THIS AGE:

- ⊙ Are very capable at using computers and cell phones (i.e., following commands, using the mouse, and playing computer games)
- ⊙ Will accept media content at face value
- ⊙ Don't have the critical thinking skills to be online or text alone
- ⊙ May be frightened by media images, both real and fictional
- ⊙ May be unintentionally exposed to inappropriate websites
- ⊙ Are vulnerable to online marketers who encourage them to give out personal information through surveys, contests, and registration forms
- ⊙ Risk moving from appropriate to inappropriate sites through hyperlinks

GUIDELINES:

- Always sit with your children when they are online.
- ⊙ If children are introduced to the Internet, parents are encouraged to:
 1. Use kid-friendly search engines and/or "walled gardens" with parental controls. (See Appendix B-8 for a list of kid-friendly search engines.)
 2. Set age-appropriate filtering at the most restrictive level.
 3. Create a personalized online environment by limiting your kids to their list of favorite or "bookmarked" sites.
 4. Keep Internet-connected computers in an open area where you can easily monitor your kids' activities.
 5. Start teaching kids about privacy. Tell them never to give out information about themselves or their family when online.
 6. Have your kids use an online nickname if a site encourages them to submit their names to "personalize" the web content.
 7. Block or disallow the use of instant messaging (IM), e-mail, chat rooms, mobile Internet, text, picture and video messaging, and access to or message boards at this age.

NOTE: Services such as The Children's Internet offer children safe, age-appropriate Internet experience available for a monthly fee. If you do allow your child to use a mobile device, use a kid-friendly mobile device (See B-16).



EIGHT- TO TEN-YEAR-OLDS

KIDS AT THIS AGE:

- ⊕ Are interested in the activities of older kids in their lives, are starting to develop a sense of their own identity, and they tend to be trusting and do not often question authority
- ⊕ Enjoy surfing online and using mobile devices for fun and playing interactive games
- ⊕ May be using e-mail and may also experiment with instant messaging (IM), chat rooms, and message boards (online forums), social networking and other interactive sites, and mobile devices although the use of these programs is strongly discouraged at this age
- ⊕ Are curious and interested in discovering new information
- ⊕ Lack the critical thinking skills to be online alone
- ⊕ Are vulnerable to online marketers who encourage them to give out personal information through surveys, contests, and registration forms
- ⊕ May be frightened by realistic portrayals of violence, threats, or dangers
- ⊕ May begin to communicate with online acquaintances they may not know in real life
- ⊕ May be influenced by media images and personalities, especially those that appear “cool” or desirable
- ⊕ May be exposed to search results with links to inappropriate websites
- ⊕ Are vulnerable to online predators if they use chat rooms, message boards, social networking, text messaging or instant messaging (IM)

GUIDELINES:

- ⊕ Sit with your kids when they are online, or make sure they only visit sites you have approved.
- ⊕ Keep any Internet-connected computer in an open area where you can closely monitor your child's online use.
- ⊕ Set parental controls at the age-appropriate levels and use filtering and monitoring tools as a complement—not a replacement—for parental supervision.
- ⊕ Use kid-friendly search engines or search engines with parental controls.
- ⊕ Do not allow instant messaging, chat rooms, or social networking sites intended for older audiences at this age. (*See Appendix B-12 for a list of social networking sites for younger children.*)
- ⊕ You and your child should have the same e-mail address. Establish a shared family e-mail account with your Internet service provider rather than letting your kids have their own accounts.
- ⊕ Get to know your child's online activities and friends. Talk to your kids about their online friends and activities just as you would about their other activities.
- ⊕ Teach your kids to always come to you before giving out information through e-mail, message boards, registration forms, personal profiles, and online contests.



ELEVEN- TO THIRTEEN-YEAR-OLDS

KIDS AT THIS AGE:

- ⊙ Can be highly influenced by what their friends are doing online and crave more independence
- ⊙ Tend to use the Internet to help with school work, to download music, e-mail others, play online games, and go to sites of interest
- ⊙ Enjoy communicating with friends by instant messaging (IM) and chat features, and text messaging on their cell phones
- ⊙ Lack the critical thinking skills to judge the accuracy of online information
- ⊙ Feel in control when it comes to technology
- ⊙ Are vulnerable to online marketers who encourage them to give out personal information through surveys, contests, and registration forms
- ⊙ Are at a sensitive time in their sexual development—particularly boys—and may look for pornographic sites. Girls may try to imitate provocative media images and behaviors.
- ⊙ Are interested in building relationships (especially girls) with online acquaintances, and are susceptible to crushes on older teens or young adults
- ⊙ Are at the most vulnerable age range to become victims of sexual predators
- ⊙ May be bullied or may be bullying others online

GUIDELINES:

- ⊙ Keep Internet-connected computers in an open area and out of your children's bedrooms.
- ⊙ Set parental controls at the age-appropriate levels and use filtering and monitoring tools as a complement—not a replacement—for parental supervision. Use parental controls on all Internet-enabled devices such as cell phones, gaming devices, iPods, and PDAs.
- ⊙ Talk with your kids about their online friends and activities just as you would about their offline activities.
- ⊙ Instruct your child to avoid face-to-face meetings with anyone they only know online. "Online friends" may not be who they claim to be.
- ⊙ Teach your kids never to give out personal information without your permission when participating in online activities (including e-mail, chat rooms or instant messaging, filling out registration forms and personal profiles, and entering online contests).
- ⊙ Insist on access and passwords to your kids' e-mail and instant messaging accounts to make sure that they're not talking to strangers. Limit instant messaging to a parent-approved buddy list.
- ⊙ Talk to your kids about ethical online behavior. They should not be using the Internet to spread gossip, bully, or make threats against others.
- ⊙ Disallow chat rooms.
- ⊙ Do periodic spot checks (like checking browser history files) to monitor your kids' online behaviors.
- ⊙ Limit time online.
- ⊙ Do not allow your children to have online profiles or pages on social networking sites that have a minimum age requirement such as MySpace (thirteen years old) and Facebook (thirteen years old). (Kids can lie about their ages and gain access to these sites.) Only allow your children to access YouTube with caution. Sites such as Imbee, ClubPenguin, and TweenLand are more appropriate for users under fourteen years of age. Follow the *Rules 'N Tools*® Parent's Guideline regarding social networking sites.
- ⊙ Your children should not post pictures or videos unless under close parental supervision.



FOURTEEN- TO EIGHTEEN-YEAR-OLDS

KIDS AT THIS AGE:

- ⊙ Crave both group identity and independence
- ⊙ Tend to download music, use instant messaging (IM), e-mail, social networking sites, and play online games; most of them have visited chat rooms, and many have participated in adult or private chat
- ⊙ May push the boundaries of safe online behavior by looking for gross humor, gore, gambling, or explicit adult sites
- ⊙ Are more critical and selective in their media interests and activities
- ⊙ Are more likely to receive unwanted sexual comments online
- ⊙ Receive the highest percentage of pornographic spam
- ⊙ Are interested in building relationships with online acquaintances (especially true of girls)
- ⊙ Are more likely to be asked for a real-life meeting by an online acquaintance, and more apt to accept
- ⊙ Are still vulnerable to online marketers who encourage them to give out personal information through surveys, contests, and registration forms
- ⊙ May be bullied or be bullying others online
- ⊙ Are more likely to use credit cards online
- ⊙ May be experimenting with online gambling

REMEMBER: A teen's prefrontal cortex is not fully developed at this age; teens still need your guidance!

GUIDELINES:

- ⊙ Create a list of Internet house rules with your teens (see *Rules 'N Tools*® Youth Pledge). You should include the kinds of sites that are off limit.
- ⊙ Set parental controls at the age-appropriate levels and use filtering and monitoring tools as a complement—not a replacement—for parental supervision. Use parental controls on all Internet-enabled devices such as cell phones, gaming devices, iPods, and PDAs.
- ⊙ Keep Internet-connected computers in an open area and out of your teens' bedrooms.
- ⊙ Talk to them about their online friends and activities just as you would about their offline activities.
- ⊙ Talk to your teens about their IM list and make sure they're not talking to strangers. Your teens should only use parent-approved buddy lists and you should check their lists regularly to make sure your teens do not alter them.
- ⊙ Insist that your teens tell you first if they want to meet an "online friend." Then check out the online friend, and if you feel the online friend is safe, accompany your child to the meeting.
- ⊙ Teach your teens to protect personal information (see *Rules 'N Tools*®).
- ⊙ Help protect them from spam. Tell your teens not to give out their e-mail address online or respond to junk mail, and to use e-mail filters.
- ⊙ Teach your teens responsible online behavior. File-sharing and taking text, images, or artwork from the web may infringe on copyright laws.
- ⊙ Talk to them about ethical behavior. They should not be using the Internet to spread gossip, bully, or threaten others.
- ⊙ Oversee financial transactions online, including ordering, buying, or selling items.
- ⊙ Discuss gambling and its potential risks, and remind your teens that it is illegal for them to gamble online.
- ⊙ Do periodic spot checks (like checking browser history files) to monitor your kids' online behaviors.

REMEMBER: Kids are safest if not on social networking sites. Follow the *Rules 'N Tools*® if you allow your teens to use them.



Rules 'N Tools®

GLOSSARY OF TERMS

Adware: A form of malicious code that displays unsolicited advertising on your computer.

Anti-virus Software: Software that attempts to block malicious programs/code/software (called viruses or malware) from harming your computer.

Blog/Blogging (short for web log): A diary or personal journal kept on a website. Blogs are usually updated frequently and sometimes entries are grouped by specific subjects, such as politics, news, pop culture, or computers. Readers often post comments in response to blog entries.

Bookmark: A saved link to a website that has been added to a list of saved links or favorite sites (i.e., "Favorites") that you can click on directly, rather than having to retype the address when revisiting the site.

Browser: A program that lets you find, see, and hear material on web pages. Popular browsers include Netscape Navigator, Safari, Microsoft Internet Explorer, Firefox, and Chrome.

Buddies (Buddy List): A list of friends a user interacts with online through various media such as instant messaging (IM) and chat.

CDA: The Communications Decency Act of 1996, a part of the Telecommunications Act of 1996, was the first attempt by the U.S. Congress to protect children on the Internet from pornography. CDA prohibited knowingly sending or displaying "indecent" material to minors through the computer, defined as: "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms of patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." The Act was immediately challenged by a law suit by the ACLU and blocked by a lower court. A year later the U.S. Supreme Court struck down the indecency provisions of the CDA in the historical cyberlaw case of *Reno v. ACLU* (1997). The Supreme Court held that a law that places a "burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving" the same goal.^{xvii} However, the court reaffirmed the application of obscenity and child pornography laws in cyberspace—an important victory for the protection of children online.

Chat Room: A location online that allows multiple users to communicate electronically with each other in real time, as opposed to delayed time as with e-mail.

^{xvii} *Reno v. ACLU*, 521 U.S. 844 (1997).



Circumventor Sites: Parallel websites that allow children to get around filtering software and access sites that have been blocked.

Closed Systems: A limited network of sites that are rated and categorized by maturity level and quality. Within a closed system, children cannot go beyond the network white list of approved websites, also referred to as a “walled garden.”

Cookie: A piece of information about your visit to a website that some websites record automatically on your computer. By using a cookie, a website operator can determine a lot of information about you and your computer. Cookies are not always bad. For example, a cookie remembers that you prefer aisle seats in the front of the plane.

COPA: The Child Online Protection Act (COPA) of 1998 was an effort by the U.S. Congress to modify the CDA in response to the Supreme Court’s decision in *Reno v. ACLU*. The law sought to make it a crime for commercial websites to make pornographic material that is “harmful to minors” available to juveniles. The purpose of COPA was to protect children from instant access to pornographic “teaser images” on porn syndicate web pages, by requiring pornographers to take credit card numbers, adult verification numbers, or access codes to restrict children’s access to pornographic material and to allow access to this material for consenting adults only. Despite the critical need for measures to protect children from accessing harmful materials, the law was immedi-

ately challenged and blocked by lower courts, and has become the subject of an epic legal battle, still raging today. The permanent injunction against the enforcement of COPA remains in effect today. The government has not announced whether it will appeal the case to the U.S. Supreme Court for a third time.

COPPA: The Children’s Online Privacy Protection Act of 1998, which went into effect in April 2000, requires websites that market to children under the age of 13 to get “verifiable parental consent” before allowing children access to their sites.^{xvii}

The Federal Trade Commission (FTC), which is responsible for enforcing COPPA, adopted a sliding scale approach to obtaining parental consent.^{xviii} The sliding scale approach allows website operators to use a mix of methods to comply with the law, including print-and-fax forms, follow-up phone calls and e-mails, and credit card authorizations.

CIPA: The Children’s Internet Protection Act (CIPA) of 2000 requires public schools and libraries receiving federal e-rate funds to use a portion of those funds to filter their Internet access. They must filter out obscenity on library computer terminals used by adults and both obscenity and harmful-to-minors materials on terminals used by minor children. CIPA was upheld by the U.S. Supreme Court as constitutional in June 2003.

^{xvii} <www.coppa.org/coppa.htm>.

^{xviii} See: Federal Trade Commission, *How to Comply with The Children’s Online Privacy Protection Rule*, November 1999. <www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm>.



Cyberbullies/Cyberbullying: Willful and repeated harm inflicted through the medium of electronic text, typically through e-mails or on websites (e.g., blogs, social networking sites).

Cybercrime: Any Internet-related illegal activity.

Cybersecurity: Any technique, software, etc., used to protect computers and prevent online crime.

Cybersex (computer sex, or “cybering”):

Refers to virtual sexual encounters between two or more persons.

Cyberstalking: Methods individuals use to track, lure, or harass another person online.

Discussion Boards: Also called Internet forums, message boards, and bulletin boards. These are online sites that allow users to post comments on a particular issue.

Domain Name: The part of an Internet address to the right of the final dot used to identify the type of organization using the server, such as .gov or .com.

Download: To copy a file from one computer system to another via the Internet (usually your computer or mobile device).

Electronic Footprint: Computers maintain a record of all website visits and e-mail messages, leaving a trail of the user’s activity in cyberspace. These data can still exist even after the browser history has been cleared and e-mail messages have been deleted.

Electronic Mail (E-Mail): An electronic mail message sent from one computer or mobile device to another computer or mobile device.

Favorite(s): The name for bookmarks (see above) used by Microsoft’s Internet Explorer browser.

File Sharing: This software enables multiple users to access the same computer file simultaneously. File sharing sometimes is used illegally to download music or software.

Filter/Filtering: Allows you to block certain types of content from being displayed. Some of the things you can screen for include course language, nudity, sexual content, and violence. Different methods to screen unwanted Internet content include whitelisting, blacklisting, monitoring activity, keyword recognition, or blocking-specific functions such as e-mail or instant messages (IM). Filtering options are available through parental control software.

Firewall: A security system usually made up of hardware and software used to block hackers, viruses, and other malicious threats to your computer.



Flame: A hostile, strongly worded message that may contain obscene language.

Gamer Tag: The nickname a user has chosen to be identified by when playing Internet games.

Gaming: Internet games, which can be played either individually or by multiple online users at the same time.

Griefers: Internet gamers who intentionally cause problems and/or cyberbully other gamers (i.e., individuals who play online games).

Grooming: Refers to the techniques sexual predators use to get to know and seduce their victims in preparation for sexual abuse.

Hardware: A term for the actual computer equipment and related machines or computer parts.

History: A tracking feature of Internet browsers that shows all the recent websites visited.

Homepage: The site that is the starting point on the web for a particular group or organization.

Identity Theft: In this crime, someone obtains the vital information (e.g., credit card, Social Security Number, bank account numbers) of another person, usually to steal money. E-mail scams, spyware, and viruses are among the most typical methods for stealing someone's identity.

Instant Message/Messaging (IM): Private, real-time text conversation between two users.

Internet (Net): A giant collection of computer networks that connects people and information all over the world.

Internet Relay Chat (IRC): A multi-use live chat facility. IRC is an area of the Internet comprising thousands of chat rooms. IRC is run by IRC servers and requires client software to use.

Internet Service Provider (ISP): A generic term for any company that can connect you directly to the Internet.

JPEG (Joint Partner Experts Group or Joint Photographic Experts Group): A popular file format for graphic images on the Internet.

Malware: Stands for malicious software or code, which includes any harmful code—trojans, worms, spyware, adware, etc.—that is designed to damage the computer or collect information.

Mobile Web: The World Wide Web as accessed from mobile devices such as cell phones, PDAs, and other portable gadgets connected to a public network. Access does not require a desktop computer.

Modem: A device installed in your computer or an external piece of hardware that connects your computer to the Internet through a phone or cable line and allows communication between computers.



Monitoring Software: Software products that allow parents to monitor or track the websites or e-mail messages that a child visits or reads.

Mouse: A small hand-controlled device for pointing and clicking to make selections on the screen.

Netiquette: Rules or manners for interacting courteously with others online (such as not typing a message in all capital letters, which is equivalent to shouting).

Password: A secret word or number that must be used to gain access to an online service or to modify software, such as a parental control.

Parental Controls: Specific features or software that allow parents to manage the online activities of children.

Peer-to-Peer (P2P) Computing: A method of sharing files directly over the Internet from one Internet-enabled device to another (computer, mobile phone, etc.), without being routed through a server.

Phishing: A scam that involves sending a fraudulent e-mail soliciting credit card, Social Security, or other personal information from an unsuspecting user.

Post: To upload information to the web.

Real Time: "Live" time; the actual time during which something takes place.

Search Engine: An Internet service that helps you search for information on the web.

Sexting: Cell phone, computer and other mobile device users—often teens and 'tweens'—create and exchange provocative messages and nude, sexual images of themselves using their cell phone's built-in digital camera and text messaging capabilities.

Skype™: A popular computer program that enables users to set up profiles, make free phone calls, chat, and video chat through their computer or mobile device from any point around the world. This free service functions through a "peer-to-peer" network, which allows individuals to communicate directly with each other rather than through a central server. Since the conversations and content exchanged through Skype are not scrutinized by monitors, children are at risk of exposure to inappropriate material and dangerous people.

SMS: Stands for "Short Message Service," a form of text messaging on cell phones, sometimes used between computers and cell phones.

Social Networks: Online communities where people share information about themselves, music files, photos, etc. There are many social networking websites (e.g., MySpace, Facebook, or Friendster).

Software: A program, or set of instructions, that runs on a computer.



Spam: Any unsolicited e-mail, or junk mail. Most spam is either a money scam or sexual in nature. Internet Service Providers, e-mail software, and other software can help block some, but not all, spam.

Spyware: A wide variety of software installed on people's computers, which collects information about you without your knowledge or consent and sends it back to whoever wrote the spyware program. The programs typically will track computer use and create numerous pop-up ads. In some instances, the spyware can damage the computer and facilitate *identity theft*.

Surfing: Similar to channel surfing on a television, Internet surfing involves users browsing around various websites following whatever interests them.

Texting: A method of sending short messages (also called SMSes, txts, or text messaging) between mobile phones and other computer-enabled devices.

Twitter: Twitter is a social media site that lets its users send short messages (or "tweets") to a network of connected users online. Twitter is similar in form to features on other social networking and instant messaging sites that allow users to update their "status" or leave an "away message" to let their friends know what they are up to in real-time, all the time. On Twitter, this is also called "micro-blogging"; individuals have 140 characters to let the world know what's on their mind or to send a tweet about something they care about.

Uniform Resource Locator (URL): The address of a site on the Internet. For example, the URL for the White House is: www.whitehouse.gov. Each URL is unique and there are millions of them.

Upload: To send information from your computer to another computer.

Username: The name a user selects to be identified on a computer, on a network, or in an online gaming forum.

Videocam (Webcam): Video cameras that are often attached to a computer so that a video image can be sent to another while communicating online.

Virus: A self-replicating software program that typically arrives through e-mail attachments and which multiplies on the hard drive, quickly exhausting the computer's memory. A trojan is a variation that allows unauthorized users access to the computer, from which they can send infected e-mails or spam.

Wireless Computers: Many networks now allow computers access to the Internet without being connected with wires. These networks are becoming increasingly more popular and powerful, allowing people to access the Internet using cell phones and other devices.

World Wide Web (WWW or Web): A hypertext-based navigation system on the Internet that lets you browse through a variety of linked resources, using typed commands or clicking on hot links.



Internet Safety 101SM

TOP 50 INTERNET ACRONYMS PARENTS NEED TO KNOW

1. **8:** it refers to oral sex
2. **1337:** it means elite
3. **143:** it means I love you
4. **182:** it means I hate you
5. **459:** it also means I love you
6. **1174:** it means nude club
7. **420:** it refers to marijuana
8. **ADR or addy:** Address
9. **ASL:** Age/Sex/Location
10. **banana:** it means penis
11. **CD9:** it means
Code 9 = parents are around
12. **DUM:** Do You Masturbate?
13. **DUSL:** Do You Scream Loud?
14. **FB:** F*** Buddy
15. **FMLTWIA:** F*** Me Like The
Whore I Am
16. **FOL:** Fond Of Leather
17. **GNOC:** Get Naked On Cam
(webcam)
18. **GYPO:** Get Your Pants Off
19. **IAYM:** I Am Your Master
20. **IF/IB:** In the Front or In the Back
21. **IIT:** Is It Tight?
22. **ILF/MD:** I Love Female/Male
Dominance
23. **IMEZRU:** I Am Easy, Are You?
24. **IWSN:** I Want Sex Now
25. **J/O:** Jerking Off
26. **KFY:** Kiss For You
27. **kitty:** it means vagina
28. **KPC:** Keeping Parents Clueless
29. **LMIRL:** Let's Meet In Real Life
30. **MOOS:** Member(s) Of the Oppo-
site Sex
31. **MOSS or MOTSS:** Member(s) Of
The Same Sex
32. **MorF:** Male or Female
33. **MOS:** Mom Over Shoulder
34. **MPFB:** My Personal F*** Buddy
35. **NALOPKT:** Not A Lot Of People
Know That
36. **NIFOC:** Nude In Front Of
Computer
37. **NMU:** Not Much, You?
38. **P911:** Parent Alert
39. **PAL:** Parents Are Listening
40. **PAW:** Parents Are Watching
41. **PIR:** Parent In Room
42. **POS:** Parent Over Shoulder
43. **PRON:** Porn
44. **Q2C:** Quick To Cum
45. **RU/18:** Are You Over 18?
46. **RUH:** Are You Horny?
47. **S2R:** Send To Receive (pictures)
48. **SorG:** Straight or Gay
49. **TDTM:** Talk Dirty To Me
50. **WYCM:** Will You Call Me?

Be sure to sign up for the E-mail Word of the Day:

www.netlingo.com/subscribe.php

 Reproduced by Permission ©1994–2008 NetLingo™ The Internet Dictionary at www.netlingo.com

INTERNET SAFETY 101SM

How to Use the DVD Series, Workbook and Rules 'N Tools® Booklet

The Internet Safety 101SM DVD teaching series and accompanying workbook are the cornerstone elements of a comprehensive program to educate, equip and empower parents, educators, and other caring adults to protect children from online dangers. The Workbook and DVD can be used alone or together and have been designed for flexible, "a la carte" use. Most of the material included is appropriate for children over the age of 16, but EIE recommends adults review the content of the DVD before showing segment elements to audiences where children are present.

Internet Safety 101SM DVD

Enough Is Enough President and renowned Internet safety expert, Donna Rice Hughes, leads a live audience in this four-part DVD teaching series. The teaching series captures the power of a live seminar, without the need for a trained facilitator, by bringing the experts to you. Video Vignettes are featured throughout this comprehensive resource, which include exclusive interviews with experts from law enforcement, industry and health care, along with poignant testimonies from kids, parents, a survivor of a sexual predator, and a convicted sex offender.

The DVD can be viewed in one sitting by pressing "Play All" or in multiple sessions by viewing individual or combined chapter segments from the DVD Menu, making it ideal for individual use or groups of any size.

DVD Components

Each of the first three segments concludes with a brief Q&A exchange between Donna, subject experts, and the live audience covering helpful, non-technical safety tips, warning signs, and conversation starters.

About Enough Is Enough

Introduction: The Perfect Storm

(viewing time: 4 minutes)

Pornography 101 (Segment 1 viewing time: 36 minutes)

Every child with unrestricted Internet access is just one click away from online pornography. Learn about the risks and how to protect children from exposure.

Predators 101 (Segment 2 viewing time: 42 minutes)

Predators and pedophiles cleverly utilize the internet to target vulnerable kids. Compelling testimonies reveal that no child is immune to the seductive tactics of a seasoned predator.

Video Vignettes (Viewing time 2 to 7 minutes each)

Each of the compelling, topical video packages featured throughout the program are also included as stand-alones, which can be used as conversation starters with friends, community members, or children. They are also an ideal tool to highlight a particular Internet concern during a community event, and can be used to promote an Internet safety event.

Web 2.0 (Segment 3 viewing time: 37 minutes)

Learn about the evolving web, the mobile internet, social networking, online gaming and cyberbullying.

Safety 101 (Segment 4 viewing time: 19 minutes)

Safety 101 is the program "take-away". Become empowered with the essential technical and non-technical safety basics (*Rules 'N Tools*®) that can be applied across all Internet-enabled devices to protect children from the dangers discussed in the first three segments.

Special Features

Includes parental control tutorials, cyber-security resources, Ad Council PSAs, and an exclusive Interview with a convicted sex offender.



Group Use

The Internet Safety 101SM program's flexibility allows groups to choose a session schedule that best meets the needs of the audience.

Groups can view all four segments of the Internet Safety 101SM DVD (total viewing time is 2 hours and 17 minutes) in one session, individually, or in various combinations. When viewing segments in separate sessions, Enough Is Enough recommends that participants begin the first session by watching *About Enough Is Enough*, followed by *Introduction: The Perfect Storm*, and then selecting one of the first three segments.

You can choose to end each group session with the final *Safety 101* segment or wait to view the safety segment after all of the first three segments have been viewed, as depicted in the Example Format on the right.

Example Format

(Each session is approximately one hour in length, before discussion)

Session 1

- *About Enough Is Enough*
- *Introduction: The Perfect Storm*
- *Segment 1: Pornography 101*
- Discussion

Session 2

- *Segment 2: Predators 101*
- *Special Features Interview: A Convicted Sex Offender Speaks Out*
- Discussion

Session 3

- *Segment 3: Web 2.0*
- *Segment 4: Safety 101*
- Discussion

Internet Safety 101SM Workbook & Resource Guide

The Workbook complements, expands upon the Internet Safety DVD, and serves as a reference tool for all of the information covered in the Internet Safety DVD.

Each of the first three segments (*Pornography 101*, *Predators 101*, and *Web 2.0*) of the workbook includes:

- ✓ **Segment Goals:** Highlights what we will cover in each segment.
- ✓ **Follow-Along/Quick-Read Section:** Includes fill-in-the-blanks, statistics, expert's quotations, helpful tips, and summary-style information covered in the DVD, which can be used while viewing the DVD.
- ✓ **A Closer Look:** Expands upon the issues covered in each segment.
- ✓ **Warning Signs:** Equips readers with vital information designed to recognize symptoms associated with the danger addressed in the segment.
- ✓ **Empowering Parents & Rules of Engagement:** Equip readers with helpful ways to discuss Internet safety with kids.
- ✓ **Discussion Questions:** Designed for a group format to encourage conversation and application.
- ✓ **How Cyber Savvy Are You?** This end-of-segment quiz is designed to test yourself to see what you learned in each segment.
- ✓ Each segment concludes with a note-taking page for your personal use.

The fourth segment, *Safety 101*, expands upon the *Safety Segment* of the DVD and comprehensively covers the Internet safety rules and software tools *Rules 'N Tools*® needed to protect children on the Internet

Appendix/Resource Guide

The Appendix and Resource Guide include information about the 101 Program, the *Rules 'N Tools*® Safety Guidelines, Checklist, Parent's Pledge, Parent Buddy Check, Youth Pledge, and Age-Based Guidelines, along with a Glossary of Terms, acronyms, resource center guides, guides on tools available, including filtering, monitoring and other parental controls, video game resources, phone devices for young users, and information from our partners and sponsors.

Rules 'N Tools® Booklet

The *Rules 'N Tools*® Booklet covers the essential technical and non-technical safety basics you need to know to protect children from online dangers, including *Rules 'N Tools*® Safety Guidelines, Checklist, Parent's Pledge, Parent Buddy Check, Youth Pledge, and Age-Based Guidelines, a Glossary of Terms and acronyms to know included in Appendix A of the workbook. Enough Is Enough recommends using the *Rules 'N Tools*® Booklet in conjunction with the Internet Safety 101SM DVD Program.

DISCLAIMERS AND LEGAL NOTICES

1. NO WARRANTIES. USE OF THE *RULES 'N TOOLS® BOOKLET* AND CONTENT IS AT YOUR SOLE RISK.

ENOUGH IS ENOUGH AND THE *RULES 'N TOOLS® BOOKLET* EXPRESSLY DISCLAIM ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. Void where prohibited by law.

2. LIMITATION OF LIABILITY. You expressly understand and agree that Enough Is Enough and the *Rules 'N Tools® Booklet* shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses (even if Enough Is Enough and the *Rules 'N Tools® Booklet* have been advised of the possibility of such damages), resulting from:

- (i) the use or the inability to use the *Rules 'N Tools® Booklet*;
- (ii) the cost of procurement of substitute goods and services resulting from any goods, data, information or services purchased or obtained from Enough Is Enough; or
- (iii) any other matter relating to the *Rules 'N Tools® Booklet*.

3. DISCLAIMER OF ENDORSEMENT. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Enough Is Enough. The views and opinions expressed herein do not necessarily state or reflect those of Enough Is Enough, and shall not be used for advertising or product endorsement purposes. This document contains links to websites maintained by other public/private organizations. These links are for information purposes only and the presence of the link does not constitute an endorsement of the site or any posted material. Although every reasonable effort has been made to present current and accurate information, Internet content appears, disappears, and changes over time. Please let us know about any existing external links that might be inaccurate or inappropriate.

