Keeping Kids Safer on the Internet

Tips for Parents and Guardians

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

OJJDP Office of Juvenile Justice and Delinquency Prevention
Office of Justice Programs ♦ U.S. Department of Justice

Keeping Kids Safer on the Internet was made possible through the joint efforts and expertise of the National Center for Missing & Exploited Children® programs noted below.

CyberTipline® is the Congressionally mandated reporting mechanism for child sexual exploitation. For more information visit www.cybertipline.com or call 1-800-843-5678.

The NetSmartz® Workshop is an online, educational resource to help teach kids how to be safer both on- and offline. For more information visit www.NetSmartz.org.

This project was supported by Grant No. 2007-MC-CX-K001 awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice. National Center for Missing & Exploited Children®, CyberTipline®, and NetSmartz® Workshop are registered service marks of the National Center for Missing & Exploited Children. NCMEC Order #168.

Copyright © 2006 and 2009 National Center for Missing & Exploited Children. All rights reserved.

Keeping Kids Safer on the Internet: Tips for Parents and Guardians is the National Center for Missing & Exploited Children's newest publication addressing Internet safety. This brochure replaces three earlier NCMEC titles — *Child Safety on the Information Highway, The CyberTipline®: Your Resource for Reporting the Sexual Exploitation of Children,* and *Teen Safety on the Information Highway.*

Special thanks to Larry Magid, author of the original *Child/Teen Safety on the Information Highway* brochures.

Allowing kids to go online without supervision or ground rules is like allowing them to explore a major metropolitan area by themselves. The Internet, like a city, offers an enormous array of entertainment and educational resources but also presents some potential risks. Kids need help navigating this world.

Where Do Kids Connect?

- Kids go online almost anywhere. They surf the Internet and send messages from a home computer or one at a friend's home, library, or school.
- Kids connect at coffee shops and other "hotspots" using laptops and wireless connections.
- Internet-enabled, video-game systems allow them to compete against and chat with players around the world.
- Wireless devices enable kids to surf the Web and exchange messages, photographs, and short videos from just about anywhere.

You can't watch your kids every minute, but you do need to use strategies to help them benefit from the Internet and avoid its potential risks.

By exploring the Internet with your kids, you greatly expand its capacity as an educational tool. By providing guidance and discussion along the way, you increase kids' online skills and confidence along with their ability to avoid potential risks. And you might be surprised by what kids teach you at the same time.

you can't take it back...

think before you type

We at the National Center for Missing & Exploited Children® (NCMEC) urge you to do one of the single most important things to promote safety — begin a dialogue with your kids about the rewards and potential risks of Internet use. We also encourage you to visit the NetSmartz® Workshop at www.NetSmartz.org and NetSmartz411℠ at www.NetSmartz411.org or call 1-888-NETS411 (638-7411) to learn more about online safety.

It's up to parents and guardians to assess the potential risks and benefits of permitting their kids to use the wide range of Internet websites and applications available. This brochure provides a list of the most popular online activities for kids along with the strategies for and benefits of reducing the potential risks associated with those activities.

According to the U.S. Department of Education, 23 percent of nursery school children in the United States use the Internet, 32 percent of kindergartners go online, and by high school 80 percent of children use the Internet.[1]

Browsing the Internet

Benefits

Browsing the Internet is like having the world's largest library and entertainment system at your fingertips. Kids are able to read stories, tour museums, visit other countries, play games, look at photographs, shop, and do research to help with homework.

Potential Risks

- Kids may come across websites containing adult images or demeaning, racist, sexist, violent, or false information.

[1] U.S. Department of Education, "Rates of Computer and Internet Use by Children in Nursery School and Students in Kindergarten through Twelfth Grade: 2003," in *Issue Brief*, October 2005, page 1, accessed February 9, 2009, at http://nces.ed.gov/pubs2005//2005111rev.pdf.

- It is hard for kids to distinguish reliable sources of information from less reliable ones. Some believe because information is posted online it must be true.

Tips to Minimize Potential Risks

- Choose search engines carefully. Some are specifically designed for kids, and others offer kid-safe options.
- Tell kids when they come across any material making them feel scared, uncomfortable, or confused to immediately tell you or another trusted adult.
- Help kids find information online. By searching the Internet together you help them find reliable sources of information and distinguish fact from fiction.

Many Internet service providers (ISPs) offer filters to prevent kids from accessing inappropriate websites. Contact your ISP about what safe-search options they offer. Remember, as a consumer you have a right to choose an ISP with the services meeting your family's needs.

Using E-mail

Benefits

Adults and kids use e-mail to communicate rapidly and cost-effectively with people all over the world. E-mail transmits messages, documents, and photographs to others in a matter of seconds or minutes.

Potential Risks

- Kids are able to set up private accounts through free Web-based, e-mail services without asking permission from parents or guardians.
- Anyone using e-mail is vulnerable to receiving "spam," messages from people or companies encouraging recipients to buy something, do

something, or visit a particular website. Spam may be sexually suggestive or offensive in other ways.

- Senders sometimes disguise themselves, pretending to be someone else — a friend or acquaintance, a well-known bank, a government agency — for illicit purposes. This is known as phishing.

Tips to Minimize Potential Risks

- Talk with your kids about their e-mail accounts, and discuss the potential risks involved. Remind them to never share passwords with anyone but you, not even their closest friends.
- Before you sign up with a service provider, research the effectiveness of its spam filters. You may also purchase spam-filter software separately.
- Teach kids not to open spam or e-mails from people they don't know in person. Remind them not to respond to any online communication in a sexually provocative way. Ask them to show you suspicious communications.
- If your kids receive e-mail containing threats or material making them feel scared, uncomfortable, or confused, report it to your service provider. Your provider's address is usually found on their home page.

Instant Messaging

Benefits

Instant Messaging (IM) allows adults and kids to have conversations in "real time" through their computer. IMing is particularly appealing to kids who use abbreviated lingo to communicate with each other. Most IM services offer a feature showing a user's contacts, known as a "buddy list," which tells the user whether a "buddy" is online and available to chat.

Potential Risks

IM is one method used to cyberbully, harass, or intimidate others. It may also be used to engage kids in a sexually explicit conversation. IM interactions may go from an innocent conversation to a sexually explicit or otherwise inappropriate exchange without warning.

Tips to Minimize Potential Risks

- Remind kids to IM only people they know in real life and who have been approved by you.
- Use privacy settings to limit contact to only those on your child's buddy list. Make sure other users cannot search for your child by his or her e-mail address and username.
- Make sure both your kids and you are familiar with the blocking features available on most IM services. Tell your kids to block any sender they don't know who IMs them.
- Take the time to learn the online lingo used by kids so you understand what they are talking about with each other.
- What's a P911? It's shorthand for "parent alert" — a code some kids use to let others know a parent or guardian is watching. If you have trouble translating your kids' online "lingo," visit www.NetSmartz.org. There you'll find a list of popular terms and abbreviations used in IM and chatrooms.

Social Networking

Benefits

Social-networking websites allow kids to connect with their friends and other users with similar interests. Kids socialize and express themselves by exchanging instant messages, e-mails, or comments and posting photographs, creative writing, artwork, videos, and music to their blogs and personal profiles.

Some 55% of online teens have profiles on a social-networking website such as Facebook or MySpace.[2]

A survey of 10 to 17 year olds revealed 34% had posted their real names, telephone numbers, home addresses, or the names of their schools online where anyone could see; 45% had posted their dates of birth or ages; and 18% had posted pictures of themselves.[3]

[2] Amanda Lenhart, Mary Madden, Alexandra Rankin Macgill, and Aaron Smith. *Teens and Social Media.* Washington, DC: Pew Internet & American Life Project, December 19, 2007, page ii, accessed February 26, 2009, at http://www.pewinternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf.

[3] Janis Wolak, Kimberly Mitchell, and David Finkelhor. *Online Victimization of Youth: Five Years Later.* Alexandria, Virginia: National Center for Missing & Exploited Children, 2006, page 50.

Potential Risks

- Some websites and services ask users to post a "profile" with their age, sex, hobbies, and interests. While these profiles help kids "connect" and share common interests, potential exploiters may pretend to be someone else and can and do use these profiles to search for victims.
- Kids sometimes compete to see who has the greatest number of contacts and will add new members to their lists even if they don't know them in person.

- Kids can't "take back" the online text and images they've entered. Kids may post information and images that are provocative and inappropriate. Once online, "chat" as well as other Web postings become public information. Anything posted online may be saved and forwarded to an unlimited number of users. Remind kids once images are posted they lose control of them and can never get them back.
- Kids have been reprimanded by their school administrators and families; denied entry into schools; and even not hired because of dangerous, demeaning, or harmful information found on their personal websites or blogs.

Tips to Minimize Potential Risks

- Urge kids to use privacy settings to restrict access to profiles so only those on their contact lists are able to view them.
- Remind kids to only add people they know in person to their contact lists.
- Encourage them to choose appropriate screennames or nicknames — such as those that refer to sports and interests, but are not sexual, violent, or offensive. Make sure the name doesn't include information revealing their identity or location.

- Visit social-networking websites with your kids, and exchange ideas about what you think is safe and unsafe.
- Ask your kids about the people they are communicating with online.
- Insist your kids never give out personal information or arrange to meet in person with someone they've met online without first checking with you.
- Encourage your kids to think before typing, "Is this message hurtful or rude?" Also urge your kids not to respond to any rude or harassing messages or ones making them feel scared, uncomfortable, or confused. Have them show you such messages.

Cellular Telephones/Wireless Devices and Texting

Benefits

Many parents and guardians look at cellular telephones as a necessity for their kids. It is reassuring to know they may reach you or call for help in an emergency. Cellular telephones/wireless devices may also be used to send text messages, images, and videos.

Potential Risks

- Cellular telephones make it easy for kids to communicate with others without their parents' or guardians' knowledge.
- Kids are increasingly using cellular telephones/wireless devices to take sexually explicit photographs of themselves and send them to their friends. Once these photographs are sent, there is no way of getting them back. In some instances children have been prosecuted for production of child pornography for taking these pictures.
- Kids may also take embarrassing or revealing photographs of others and post them to the Internet, leaving victims few options to defend or protect themselves from this form of bullying.

Tips to Minimize Potential Risks

- Create rules about the appropriate use of cellular telephones/wireless devices and set limits, including who your kids may communicate with and when they may use their cellular telephones/wireless devices
- Review cellular-telephone/wireless-device records for any unknown numbers and late-night telephone calls
- Teach your kids to never post their cellular telephone number anywhere online
- Talk to your kids about the possible implications of sending sexually explicit or provocative images of themselves or others
- Think about removing the Internet features from your kid's cellular telephone/wireless device through your service provider or consider creating settings to control or prohibit access to the Internet, e-mail, or text messaging

Posting Videos and Photographs Online

Benefits

Webcams, cellular telephones, and digital cameras allow kids to post videos, photographs, and audio files online and engage in video conversations. Kids often use this equipment to see each other as they IM and chat.

Webcams are often used to help kids stay in touch with family members and friends including traveling parents and guardians and those living in other areas.

Potential Risks

- Webcam sessions and photographs may be easily captured and saved, and users may continue to circulate those images online. In some cases people believed they were interacting with trusted friends but later found their images were distributed to others or posted on websites.
- Capturing, sending, and posting sexually provocative and inappropriate images may lead to legal implications and other unexpected offline consequences.

Tips to Minimize Potential Risks

- Kids should use webcams or post photographs online only with your knowledge and supervision.
- Remind your kids to ask themselves if they would be embarrassed if their friends or family members saw the pictures or videos they post online. If the answer is yes, then they need to stop.
- Remind kids to be aware of what is in the camera's field of vision and remember to turn the camera off when it is not in use.
- Caution kids about posting identity-revealing or sexually provocative photographs. Don't allow them to post photographs of others — even their friends — without permission from their friends' parents or guardians. Remind them once such images are posted they lose control of them and can never get them back.

Online Gaming

Benefits

Online gaming involves playing a game over a computer network, often on the Internet, or Internet-enabled game console. Online gaming allows kids to engage with and challenge players from around the world. Many online games have text, chatroom, or IM functions, allowing players to communicate as a group or in private. Some even allow users to speak directly to each other using voice-enabled headphones. In addition online games often have associated online communities for players to share experiences and strategies. In many ways online games and gaming communities serve as a forum for social networking.

Potential Risks

- There is never any guarantee your kid is communicating with other kids, those they know in person, or those approved by you

- As with IM or social-networking websites, kids may be exposed to inappropriate language, harassed, threatened, or asked sexually explicit questions

Tips to Minimize Potential Risks

- Keep the gaming console and computer in a common area of the home so you are able to more easily supervise
- Set rules, including how long your kids may play, who they are allowed to play with, and what types of games are appropriate
- Check out rating systems to help you decide which games to allow in your home
- Look into what types of protections or parental controls the gaming console allows and make use of them

Other Ways to Enhance Kids' Online Safety Skills

Begin a Dialogue With Your Kids About Internet Use

Because we use the Internet in different ways, kids and adults may learn from each other. By talking about Internet use with your kids, you are opening the door to discussing the important issues of personal safety and helping them engage in responsible behavior. Use this brochure as a starting point, or visit www.NetSmartz.org to find safety resources for both kids and adults.

Consider Rating, Blocking, Monitoring, and Filtering Applications for Your Computer

Software and services are available to help parents and guardians set limits on kids' Internet use. Most computer-operating systems have optional filters allowing parents and guardians to block websites they consider inappropriate. Some services rate websites

for content. Some programs prevent users from entering information such as names and addresses, and others keep kids away from chatrooms or restrict their ability to send or read e-mail. Monitoring programs allow you to see where your kids go online. But remember these programs and services don't develop kids' own sense of safety, and they are not substitutes for parental/guardian communication, supervision, and involvement.

Make Internet Use a Family Activity While Encouraging Critical Thinking

By setting aside time to go online with your kids you not only become more aware of what they do online, you reinforce positive Internet skills. Helping your kids with a research project is a great opportunity for them to learn about and distinguish which websites provide reliable information, are simply someone's opinion, and are to be avoided entirely. And when looking at e-mails together ask, "Are these people who they seem to be?" These are prime opportunities to help kids develop their critical-thinking skills.

Set Reasonable Rules

Work with your kids to develop reasonable rules. Consider setting rules about the time of day, length of time, people they may communicate with, and appropriate areas for them to visit while online. Also explain to your kids why these rules are important.

Encourage Your Kids to Go to You When They Encounter Problems Online

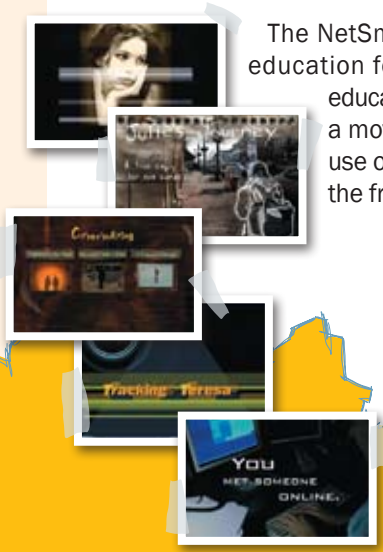
It's important to reassure kids if they encounter problems online or view something disturbing, it's not their fault. Discussing these issues openly may reduce their fear of going to you if they encounter something online making them feel scared, uncomfortable, or confused. Be a resource. Let them know if they share the experience with you, you will try to help, not punish, them. At the same time help them understand what happened and avoid similar situations in the future.

Online Resources for Families

NetSmartz® Workshop

The NetSmartz Workshop is an online, educational resource for kids of all ages and their trusted adults to help foster positive choices when on the Internet and in the real world.

The NetSmartz program is designed to be used in homes, schools, and communities. It provides parents, guardians, educators, community leaders, and law-enforcement officials with a wide variety of resources including activities, games, presentations, safety pledges, and videos. These resources help trusted adults build kids' safety awareness, prevent their victimization, and increase their self-confidence on- and offline.



The NetSmartz Workshop is a leader in safety education for youth, parents and guardians, and educators. The program was created to spearhead a movement toward safer and more responsible use of the Internet by kids and teens. Download the free resources at www.NetSmartz.org.

kids
parents
teens
educators
tweens
community leaders
guardians
law-enforcement officials

NetSmartz411

NetSmartz411 is a free, first-of-its-kind service provided by the National Center for Missing & Exploited Children and funded by the Qwest Foundation. It was designed to raise Internet-safety awareness and provides general information about computers and the Web.

Parents, guardians, and educators are able to find this resource at www.NetSmartz411.org. The website contains a searchable knowledgebase of frequently asked questions regarding computers and the Internet, along with the opportunity to ask questions of experts. Questions may be submitted via the website anytime or called into experts at 1-888-NETS411 (638-7411), Monday through Friday, from Noon to 8:00 P.M., EST.

CyberTipline

Visit www.cybertipline.com or call 1-800-843-5678 to report the sexual exploitation of children on- and offline. The CyberTipline accepts information about the possession, manufacture, and distribution of child pornography; online enticement of children for sexual acts; child victims of prostitution; sex tourism involving children; extrafamilial child sexual molestation; unsolicited obscene material sent to a child; misleading domain names, and misleading words or digital images on the Internet. Your information will be forwarded to law enforcement and Internet service provider(s) for investigation and review when appropriate.

Don't Believe the Type

Created by the Ad Council and NCMEC, "Don't Believe the Type," is part of a public-service campaign specifically designed to help teens recognize the dangers of the Internet, situations to avoid, and how to "surf safer." Visit www.cybertipline.com, and click on the "Don't Believe the Type" link to view the website.

Think Before You Post

A part of NCMEC's Ad Council public-service campaign, "Think Before You Post" is a public-service campaign warning kids about the dangers of posting inappropriate pictures and videos of themselves online. Visit www.cybertipline.com and click on the "Think Before You Post" link to view the website.

Tips for Parents and Guardians

- Begin a dialogue with your kids about safe Internet use and supervise their online activities
- Consider rating, blocking, monitoring, and filtering applications for your computer
- Make Internet use a family activity
- Encourage your kids' critical-thinking skills
- Set reasonable rules for going online
- Encourage your kids to tell you when they encounter problems online
- If they come across lewd, obscene, or illegal material or if they are contacted by someone who attempts to engage them in sexual conversation, make a report to NCMEC's CyberTipline at www.cybertipline.com or 1-800-843-5678

Find More Help Online

Visit www.NetSmartz.org for a wealth of additional safety resources including

- Family-discussion starters about online and real-world safety
- A blog about current and developing Internet and real-world safety issues
- Informative statistics about kids' Internet use
- Tips for addressing risks to kids on- and offline
- Commonly used chat abbreviations and acronyms
- At-home activities for talking about safety during teachable moments

Visit www.NetSmartz411.org for answers to commonly asked questions about the Internet, computers, or the Web or to ask specific questions of experts

Help Us Promote a Safer Internet

If you have information to help NCMEC in the fight against child sexual exploitation, please report it to the CyberTipline at www.cybertipline.com or 1-800-843-5678.