Child Safety on the Information Highway

www.missingkids.com
www.cybertipline.com

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

US ISPA
US Internet Service Provider Association

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

"Cyberspace," the "web," the "net," the "information highway," whatever it's called, millions of people are now going online to exchange electronic mail (E-mail) and instant messages; participate in chat groups; post and read messages in newsgroups, which are sometimes called bulletin boards; "surf" the world wide web; and many other online activities. Children are no exception and in fact are more likely to be online than adults.

Personal computers are no longer the only method used for accessing the Internet. Children can go online from personal computers at home, at a friend's house, in school, at a library, at a club, or at a cafe. Many game consoles can be connected to the Internet and used for chatting and other online interaction. It is also possible to access the Internet using mobile devices such as cellular telephones and other handheld devices. In other words children don't have to be in the company of responsible adults to use the Internet.

To get online you can sign up with an Internet Service Provider (ISP), which will provide you with access to web sites and other areas of the Internet. Most people get online by using high-speed broadband connections such as a Direct Subscriber Line (DSL) or cable modems, but many families are still using a modem to connect their computer to a telephone line. Most cellular telephones sold today come with a web browser, E-mail, and some form of instant or "short" messaging system (SMS).

Even though ISPs and cellular telephone companies strive to provide their subscribers with an enjoyable, safe, and rewarding online experience, it's not possible for these companies to monitor everyone who uses their service anymore than a



local government can control the behavior of the people within its borders. Once you're connected to the Internet you're able to exchange information with people who use other ISPs and online services unless you're using a service offering restricted access such as blocking mail from outside the service or from people who aren't pre-approved by a child's parent or guardian.

There are no censors on the Internet. Anyone in the world — companies, governments, individuals, and organizations — can publish material on the Internet. An ISP links you to these sites, but it can't control what is on them. It's up to individuals to make sure they behave in a safe and appropriate way.

Benefits of the Information Highway

There is a vast array of services available online. **Reference information** such as airline fares, encyclopedias, movie reviews, news, sports, stock quotes, and weather are readily available. Users can conduct **transactions** such as banking, making travel reservations, shopping, and trading stocks online. You can find information about your local schools, government, and vital health matters. You can read an out-of-town newspaper online. Millions of people **communicate** through E-mail with family, friends, and colleagues around the world. Other people use chat areas to communicate with those who have common interests. You can even use the Internet to watch videos and listen to audio programs produced by major media companies, businesses, organizations, and individuals.

It's up to individuals to make sure they behave in a safe and appropriate way.

As an **educational and entertainment tool** users can learn about virtually any topic, visit a museum, take a college course, or play an endless number of computer games with other users or against the computer itself.

Most people who go online have mainly positive experiences. But, like any endeavor — attending school, cooking, riding a bicycle, or traveling — there are some risks and annoyances. The online world, like the rest of society, is made up of a wide array of people. Most are decent and respectful, but some may be rude, obnoxious, insulting, or even mean and exploitive. Children get a lot of benefits from being online, but they can also be targets of crime, exploitation, and harassment in this as in any other environment. Trusting, curious, and anxious to explore this new world and the relationships it brings, children need supervision and common-sense advice regarding how to be sure their experiences in "cyberspace" are happy, healthy, and productive.

As an educational and entertainment tool users can learn about virtually any topic....

Putting the Issue in Perspective

There have been some highly publicized cases of exploitation involving the Internet, but that doesn't mean every child will experience major problems. The vast majority of people who use the Internet do not get into serious trouble. Many people, including children, have been confronted with disturbing or inappropriate material. There are steps parents and guardians can take to try to shield their children from such material, but it's almost impossible

to completely avoid all inappropriate material. Sadly there are some cases where children have been victimized by serious crime as a result of going online. Families can greatly minimize the chances their children will be victimized by teaching children to follow the safety rules on the back cover. **The fact that crimes are being committed online, however, is *not* a reason to avoid using these services.** To tell children to stop using the Internet would be like telling them to forgo attending school because students are sometimes victimized or bullied there. A better strategy would be to instruct children about both the benefits and dangers of "cyberspace" and for them to learn how to be "street smart" in order to better safeguard themselves in any potentially dangerous situation.

...Instruct children...to be "street smart"...to better safeguard themselves...

What Are the Risks?

There are a few risks for children who use the Internet or other online services. Teenagers are particularly at risk because they often go online unsupervised and are more likely than younger children to participate in online discussions regarding companionship, relationships, or sexual activity. If you have a teen in your family or you are a teenager, check out *Teen Safety on the Information Highway* at the "More Publications" link of www.missingkids.com or order a free copy by calling 1-800-843-5678.

Teenagers are particulary at risk because they ...are more likely... to participate in online discussions regarding companionship....

Some specific risks include

- **Exposure to inappropriate material.** Your child may be exposed to inappropriate material considered to be sexual, hateful, or violent in nature or material encouraging dangerous or illegal activities. Children could seek out such material but may also come across it on the web via chat areas, E-mail, or even instant messaging if they're not looking for it.
- **Physical molestation.** Your child might provide information or arrange an encounter possibly risking his or her safety or the safety of other family members. In some cases child molesters have used chat areas, E-mail, and instant messages to gain a child's confidence and then arrange a face-to-face meeting.
- **Harassment and bullying.** Your child might encounter messages via chat, E-mail, or their cellular telephones that are belligerent, demeaning, or harassing. "Bullies," typically other young people, often use the Internet to bother their victims.
- **Viruses and hackers.** Your child could download a file containing a virus that could damage the computer or increase the risk of a "hacker" gaining remote access to the computer. This could jeopardize your family's privacy and safety.
- **Legal and financial.** Your child could do something that has negative legal or financial consequences such as giving out a family member's credit-card number or doing something violating another person's rights. Legal issues aside, children should be taught good "netiquette" which means to avoid being inconsiderate, mean, or rude on the Internet.



How Families Can Reduce the Risks

While children need a certain amount of privacy, they also need family involvement and supervision in their daily lives. The same general "parenting" skills that apply to the "real world" also apply online.

If you have cause for concern about your children's online activities, talk to them. Also seek out the advice and counsel of teachers, librarians, and other Internet and online service users in your area. Having open communication with your children, using computer resources, and getting online yourself will help you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use. If your child tells you about an upsetting message, person, or web site encountered while online, don't blame your child but help him or her avoid problems in the future. Remember — how you respond will determine whether they confide in you the next time they encounter a problem and how they learn to deal with problems on their own.

While children need a certain amount of privacy, they also need family involvement....

Beyond these basics there are some specific things you should know about the Internet. For instance did you know there are chat areas, newsgroups, and web sites that have hateful or violent material or material otherwise considered to be inappropriate by parents or guardians? It's possible for children to stumble across this type of material when doing a search using one of the web sites specifically designed to help people find

information on the Internet. Most of these sites, called "search engines," do not, by default, filter out material that might be inappropriate for children, but some offer a child-safe option and others are designed specifically for use by children. Remember, finding inappropriate material online can make people feel badly or even hurt people. If your children end up in any of these areas, tell them to immediately leave by clicking on the Home icon, going to another site, or shutting down the browser.

Also the Internet contains newsgroups, web sites, and other areas designed specifically for adults who wish to post, read, or view sexually explicit material including pictures, stories, and videos. Some of this material is posted on web sites where there is an attempt to verify the user's age and/or a requirement for users to enter a credit-card number on the presumption that children do not have access to credit-card numbers. Other areas on the Internet make no such effort to control access. Nevertheless, consider monitoring your credit-card bills for such charges. In addition to "adult" pornography, there are also areas on the Internet containing illegal pornographic images of children. If you or your children come across this type of material, immediately report it to the National Center for Missing & Exploited Children's (NCMEC) CyberTipline® at www.cybertipline.com.

Report pornographic images of children to the National Center for Missing & Exploited Children's CyberTipline at www.cybertipline.com

Some online services and ISPs allow parents or guardians to limit their children's access to certain services and features such as adult-oriented "chatrooms," bulletin boards, and web sites. There

may be an area just for children where it is less likely for them to stumble onto inappropriate material or get into an unsupervised "chatroom." At the very least, keep track of any files your children download to the computer, consider sharing an E-mail account with your children to oversee their mail, and consider joining them when they are in private chat areas.

In addition there are ways to filter or control what your children can see and do online. One type of filter, called a "spam" filter, limits unsolicited E-mail including mail promoting sexually explicit material. Some ISPs and E-mail services include filters as part of their service but, if not, there is software you can purchase that will attempt to limit the type of mail getting through.

There are also ways to filter what a child can see on the world wide web. Check with your service provider to see if they offer age-appropriate "parental controls." If not consider using a software program blocking chat areas, newsgroups, and web sites known to be inappropriate for children. Most of these programs can be configured by the parent or guardian to filter out sites containing nudity, sexual content, hateful or violent material or advocating the use of alcohol, drugs, or tobacco. Some can also be configured to prevent children from revealing information about themselves such as their name, address, or telephone number. You can find a directory of these filtering programs at http://kids.getnetwise.org/tools.

Another option is to use a rating system that relies on web-site operators to indicate the nature of their material. Internet browsers can be configured to only allow children to visit sites rated at the level parents or guardians specify. The advantage to this method is only appropriately rated sites can be

viewed. The disadvantage is many appropriate web sites have not submitted themselves for a rating and will therefore be blocked.

While technological-child-protection tools are worth exploring, they're not a panacea. To begin with, no program is perfect. There is always the possibility something inappropriate could "slip through" or something appropriate will be blocked. Finally, filtering programs do not necessarily protect children from all dangerous activities. For example some do not control instant messaging or chat services, which are particularly dangerous because they put a child in instant communications with other people. Also some filters do not work with peer-to-peer networks allowing people to exchange files such as music, pictures, text, and videos. These peer-to-peer networks are sometimes used to distribute pornography, including pornographic images of children. And file-sharing when in peer-to-peer networks may turn your personal computer into a server that shares your files, which can place you in legal trouble or possibly allow others to gain access to your child's personal stuff on his or her computer. It's like giving someone you don't know the opportunity to know everything. Thus filters are not a substitute for family-member involvement.

Regardless of whether you choose to use a filtering program or an Internet rating system, the best way to assure your children are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with your children while they're online. Have them show you what they do, and ask them to teach you how to use the Internet or online service. You might be surprised by how much you can learn from your children.



Guidelines for Parents or Guardians

By taking responsibility for your children's online computer use, parents or guardians can greatly minimize any potential risks of being online. Make it a family rule to

- Never give out identifying information — home address, school name, or telephone number — in a public message such as chat or newsgroups, and be sure you're dealing with someone both you and your children know and trust before giving out this information via E-mail. Think carefully before revealing any personal information such as age, financial information, or marital status. Do not post photographs of your children in newsgroups or on web sites available to the public. Consider using a pseudonym, avoid listing your child's name and E-mail address in any public directories and profiles, and find out about your ISP's privacy policies and exercise your options for how your personal information may be used.

Have your child show you what he or she does online, and become familiar with all the activities available online.

- Get to know the Internet and any services your child uses. If you don't know how to log on, get your child to show you. Have your child show you what he or she does online, and become familiar with all the activities available online. Find out if your children have a free web-based, E-mail account, such as those offered by some ISPs. If so learn their user names and passwords on those accounts. Also learn the places, such as school and the library, where they can access those accounts.

- Never allow your child to arrange a face-to-face meeting with someone they first "meet" on the Internet without an adult family member's permission. If a meeting is arranged, make the first one in a public place, and be sure to accompany your child.

If a meeting is arranged, make the first one in a public place, and be sure to accompany your child.

- Never respond to messages that are suggestive; are obscene; are belligerent; are threatening; or make you feel scared, uncomfortable, or confused. Encourage your children to tell you if they encounter such messages. If you or your child receives a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your ISP, and ask for their assistance. Instruct your child **not** to click on any links contained in E-mail from persons they don't know. Such links could lead to sexually explicit or otherwise inappropriate web sites or could be a computer virus.

Remember people online may not be who they seem to be.

If someone sends you or your children messages or images that are indecent, lewd, or obscene with the intent to abuse, annoy, harass, or threaten you, or if you become aware of the transmission, use, or viewing of pornographic images of children while online, immediately report this to NCMEC's CyberTipline at 1-800-843-5678 or www.cybertipline.com.

- Remember people online may not be who they seem. Because you can't see or even hear the person it would be easy for someone to misrepresent him- or herself. Thus someone indicating "she" is a "12-year-old girl" could in reality be a 40-year-old man.
- Remember everything you read online may not be true. Any offer that's "too good to be true" probably is. Be careful about any offers involving you going to a meeting, having someone visit your home, or sending money or credit-card information.
- Set reasonable rules and guidelines for computer use by your children. *See* "My Rules for Online Safety" on the back cover, discuss them with your children, and post them near the computer as a reminder. Remember to monitor your children's compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child's excessive use of online services or the Internet, especially late at night, may be a clue there is a potential problem. Remember personal computers and online services should not be used as electronic babysitters.

Set reasonable rules and guidelines for computer use by your children.

- Check out blocking, filtering, and ratings applications to see if they will be of assistance to your family.

Be sure to make this a family activity. Consider keeping the computer in a family room rather than the child's bedroom. Get to know their "online

friends" just as you get to know all of their other friends. If your child has a cellular telephone, talk with him or her about using it safely. The same rules that apply to computer use also apply to the use of cellular telephones.

This brochure was written by Lawrence J. Magid, a syndicated columnist and technology commentator, who is author of *The Little PC Book* (Peachpit Press) and host of www.safekids.com, a web site devoted to keeping children safer in "cyberspace." He is also the author of *Teen Safety on the Information Highway*, a free brochure also published by the National Center for Missing & Exploited Children.

The first edition of this brochure was created with the generous sponsorship of America Online®, CompuServe®, Delphi™ Internet, e•World, GEnie®, Interchange™ Online Network, and Prodigy® Services.

This project was supported by Grant No. 2005-MC-CX-K024 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®, 1-800-THE-LOST®, and CyberTipline® are registered service marks of the National Center for Missing & Exploited Children.



For more information regarding child safety,
please contact the

Charles B. Wang International Children's Building
699 Prince Street
Alexandria, Virginia 22314-3175
1-800-THE-LOST®
(1-800-843-5678)
www.missingkids.com
www.cybertipline.com

Tear off and keep this pledge at your computer.

My Rules for Online Safety

- I will not give out personal information such as my address, telephone number, parents' or guardians' work address/telephone number, or the name and location of my school without my parents' or guardians' permission. I will not give out my Internet password(s) to anyone — even my best friends — other than my parents or guardians.
- I will tell my parents or guardians right away if I come across any information that makes me feel scared, uncomfortable, or confused.
- I will never agree to get together with someone I first "meet" online without checking with my parents or guardians. If they agree to the meeting, I will be sure it is in a public place and bring my parent or guardian along.
- I will never send a person my picture or anything else without first checking with my parents or guardians.
- I will not respond to any messages that are mean or in any way make me feel scared, uncomfortable, or confused. It is not my fault if I get a message like that. If I do I will tell a trusted adult right away so they can contact the online service.
- I will talk with my parents or guardians so we can set up rules for going online. We will decide upon the time of day I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.
- I will practice good "netiquette" by not hurting other people or breaking the law.