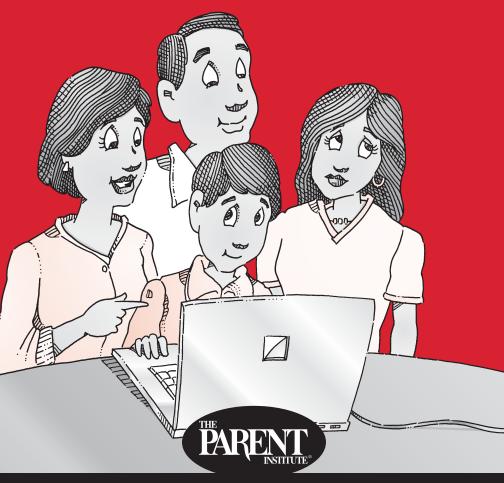
Internet Safety

& Responsibility for Students



A Guide for Parents



ou may love it, hate it or fear it, but the Internet is one thing you can't ignore. For better or worse, the Internet—with its endless possibilities and dangers—is here to stay. Your child is using it—and you need to take it seriously!

Millions of kids in all age groups are online every day—at home, at school, at friends' homes, at the library—and many are creating online content. In other words, kids aren't just using the Internet—they're *contributing* to it.

As a parent, how can you keep your child safe online while still letting him* benefit from the power of the Internet? Read this booklet to find out. You'll discover tips for safer surfing, ideas for navigating through cyberspace without getting lost, and definitions to help you make sense of all the confusing "net lingo" your child knows so well.

computers have become the most empowering tool we've ever created. They're tools of communication, they're tools of creativity, and they can be shaped by their user.

—Bill Gates

But remember: Although this booklet can help you teach your child about Internet safety, it's no substitute for good communication between you and your child or for clear, consistent rules regarding computer use.

Note: Every child is unique, so we often use the singular pronoun. We alternate using "he" and "she" throughout this booklet.





Quiz

How savvy are you when it comes to Internet safety?

Take this quiz to find out how much you know—or don't know—about your child's well-being online.

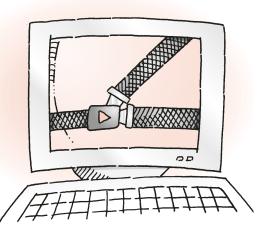
- **1.** The best place to keep our home computer is:
 - **a.** In the family room.
 - **b.** In my child's bedroom.
 - **c.** In my home office.
- 2. How can I best keep my child safe online?
 - **a.** By insisting she use the Internet in a public place like the library.
 - **b.** By not letting her surf alone.
 - **c.** By supervising her Internet usage and posting clear rules about computer use near the monitor.
- 3. Kid-friendly chat rooms are completely safe.
 - **a.** True
 - **b.** False
- **4.** Which of the following is the riskiest screen name?
 - **a.** SweetLilGrrl
 - b. Kristi_nyc1994
 - **c.** TeddyBearLvr
- **5.** According to a recent study, how many kids were sexually solicited online during a one-year period?
 - **a.** 1 in 5,000
 - **b.** 1 in 500
 - **c.** 1 in 5

(See answers on page 12.)

Keeping Your Child Safe Online

No matter what your child's age, some Internet rules always apply. These include:

- No computer in your child's bedroom. Keep it out in the open.
- No posting personal information—like last names—online.
- No choosing email addresses or screen names that are provocative and reveal your child's identity.
- No arranging face-to-face meetings with online "friends."



If your child is in elementary school, other appropriate rules include:

- No random surfing. Visit parent-approved sites only.
- No uploading or downloading files without permission.
- No clicking on pop-up ads or visiting adult chat rooms.
- No secrets. If he sees something upsetting, he must tell you.

If your child is in middle or high school, your rules should center on:

- Consistency. Continue reinforcing basic safety rules.
- Honesty. Let your older child know that you expect him to be truthful about what he's doing online and to report trouble.
- Respect. Accept his natural curiosity and desire for freedom. Don't ban the computer forever if he slips up once.

Screen name: The nickname by which a user is identified online.

Surfing: Randomly "looking around" the Internet.

Uploading: Sending data from one computer to another, or from a computer to an Internet site.

Downloading: Retrieving material from a website or another computer.

Pop-up: A random ad that appears on the screen while the user is online.

Chat room: A place on the Internet where users communicate in real time by typing messages to one another. Also called an "online forum."



Using Parental-Control Programs

ilters can help you to limit your child's exposure to Internet pornography and other disturbing material. And you may also wish to install filtering software that monitors her actions online or limits her computer usage (see "Tools that Can Help" on page 12).

However, none of these programs is foolproof, and none will teach your child to use the Internet responsibly. That's your job—which is why you should talk to her often about staying safe online. As always, you are your child's first, best and most powerful teacher.



A Note about Cell Phones and PDAs

hink cell phones are just phones? Think again. Today's cell phones (and PDAs) are like mini computers. Most have web browsers and can send instant messages and email. In light of that, many of this booklet's safety tips apply to your child's cell phone and PDA use, too.

Filtering software: Programs parents can install to screen Internet content and block access to inappropriate sites.

PDA: Personal Digital Assistant—a handheld device that can function as a phone, browser and personal organizer.

Browser: A program (such as Apple Safari™, Microsoft Internet Explorer® or Mozilla Firefox®) that helps users navigate the Internet.

Instant message (IM): An application that lets users send and receive online text messages nearly in real time. It also notifies users when friends have logged on or off.

A Closer Look at the Big Three:

Instant Messaging, Social-Networking/ Blogging Sites and Chat Rooms

1. What is Instant Messaging?

Instant messaging (IM) is a wildly popular way for kids to communicate. Think of it as "talking on the phone" by typing on the computer. As soon as one user types a message and clicks "send," the message appears on another user's screen. That user then replies, and so on. When the session ends, the messages disappear, although some applications do save chat transcripts.

With IM, users identify themselves by screen names and can communicate with friends on their "Buddy List." They can also create online profiles through which anyone can "meet" and IM them.



The attraction of IM is obvious: It's fast, free and easy. It's also widespread—if your child claims that all his friends IM, he's probably telling the truth. (To decipher what they're saying when they IM, see "Know the Shorthand" on page 12.)

If you decide to let your child IM, be sure he:

- **Chooses a screen name** that keeps his identity secret.
- Communicates only with friends you know who are on his buddy list.
- Doesn't respond to flaming and tells you about it right away.
- Understands that his messages aren't truly private.
- Applies privacy settings that make his identity visible only to friends.

Buddy List: A list of the screen names of people with whom a user regularly communicates.

Flaming: Purposely posting a cruel or inflammatory message (via IM, email or chat). Flames often come in response to prior postings.



2. Why Are Children Obsessed with Social-Networking & Blogging Sites?

It's no exaggeration: Social-networking sites (such as MySpace®, Xanga® and Facebook®) have changed the way kids connect. Through these free sites, users can send messages, blog, share files, play games and chat. Social-networking sites allow kids to communicate easily with friends. They help kids feel like part of a community. The blog option gives kids a creative outlet for expressing themselves and helps build their writing skills.

There are risks, however. Kids can also get into serious trouble. The dangers of social-networking sites include:

- Talking online with pedophiles and other criminals posing as peers.
- Being lured into face-to-face meetings with dangerous people.
- Being exposed to sexually explicit or violent material.
- Being a victim of cyberbullying.

If you've decided to let your child use social-networking sites, help her stay safe while she's logged on. (And even if you've banned such sites at home, be aware that she may have access to them at school or the library.)



If you allow your child to register with a social-networking site, be sure she:

- Agrees to stay anonymous by choosing a screen name that does NOT contain information such as her birth year or hometown.
- Restricts access to her blog so that only friends may view it.
- Knows not to post photos identifying herself or her family and friends.
- Agrees to be honest about her age and not pretend to be older.

Blog/blogging: A "web log" or journal that users post online. Bloggers usually update their sites often, and these sites may contain photos, music, videos and links. Blogging is the act of creating/maintaining a blog.

Cyberbullying: Sending or posting cruel or harassing messages online.



3. What Goes on in Chat Rooms?

According to the National Center for Missing & Exploited Children, "chat is probably the most dangerous area on the Internet." Why? Because it allows kids to "talk" with literally anyone in the world.

What's a chat room? It's an online forum where users have live conversations via text. Chat rooms are found across the Internet, including on social-networking sites. As a user types a message, others can see it and respond. Although some chat rooms are moderated, others aren't. And even in moderated rooms, users can split off for private chats.

Unfortunately, children and pedophiles seek out chat rooms for the same reason: Where better to meet an ever-changing group of kids? Still, chat rooms can give kids a chance to interact with interesting, decent people and share ideas. The key to avoiding trouble is to chat wisely.

If you permit your child to chat, insist that he:

- **Choose a nonspecific,** gender-neutral screen name.
- Never reveal identifying details about himself.
- **Stick with kid-friendly chat rooms** (though this is no guarantee that other users aren't merely posing as kids).
- Report abusive posts to the chat room's moderator, if possible.
- **Be wary of overly sympathetic** or "too nice" fellow chatters. Talk with your child about the other participants in the chat rooms he visits. Who is he chatting with? What kinds of topics are they discussing?

Remember: Keep the computer where you can observe your child's online activities!

Chat/chatting: Having a live conversation by typing messages to others. These messages are then displayed in a chat room or privately.

Cyberbullies

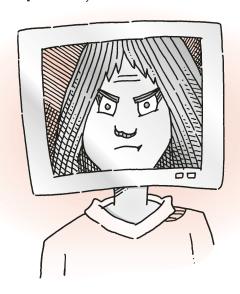


ou walk by the computer when your child is online. The message on the screen uses words that are cruel and threatening.

Bullying has moved from the schoolyard and the classroom to computers and cell phones. Kids set up blogs, then write vicious and rude messages. They post cruel and sometimes altered pictures. They trick other kids into revealing personal and often sensitive or embarrassing information, then forward it to others. Whether through chat rooms, email, IM, text messages or photos—cyberbullying is a real concern!

To help your child with this distressing situation:

- Make sure the computer is always located where you can monitor what your child is doing online.
- Let her know she can talk to you if she receives a message from a cyberbully.
- Tell your child <u>never</u>, <u>ever</u> to respond.
- Save any messages from a cyberbully.
- Alert your child's school to the problem.
- **Contact the police** if your child is threatened.



Text message: A short, typed message sent from one cell phone to another.

File Sharing

lso known as peer-to-peer (P2P) programs, file sharing programs let users swap files via the Internet. Among teens, these programs are often used to share music, pictures and videos.



The pitfalls of file sharing may include:

- **Illegality.** Sharing certain files may violate copyright laws.
- **Exposure to pornography** or other disturbing material.
- Making all of a computer's files (even private ones) available to others by mistake.
- **Exposure to viruses** or spyware.

To ensure that your child shares files safely, make sure she:

- **Never uploads** or downloads materials illegally.
- **Reads the fine print** when setting up a file-sharing program.
- Only shares files with people she knows and trusts.

Gaming

nline games are sophisticated, fun and often free, so it's no wonder kids enjoy them. But they have their drawbacks, too. Some games, for instance, contain sexual or violent content or profanity, and too much game-playing may impact your child's schoolwork.

To keep your child out of gaming-related trouble, be sure you:

- **Know what she's playing.** If something is inappropriate, either forbid it or block it (with software or through your ISP).
- **Enforce time limits.** Don't let her play until her eyes glaze over.

File sharing: Accessing another computer's files (music, video, etc.) from your computer or allowing another user to access your files.

Virus: An often destructive program that enters your computer via email or the Internet. **Spyware:** Programs that "spy" on your Internet-usage habits and report those data to a company or organization.

Software: A catch-all name for computer programs.

ISP (Internet Service Provider): A company that provides Internet access (examples include AOL® and EarthLink™).

School-Related Research

ot all Internet sites are dangerous to your child's well-being. However, some sites are full of questionable content—a big problem if your child is doing online research for school.

To keep your child from being duped by less-than-reputable sites, teach him to use reliable, kid-friendly search engines such as Yahooligans!® and Awesome Library. Also encourage him to ask himself whether a site:

- Is selling something.
- Seems "off" (is full of typos or strange grammar, for example).

When doing online research, make sure your child follows school guidelines. Remind him to:

- Cite his sources. He should include the author's name (if available), along with the site's name and URL.
- Use multiple sources and citations.
- Note the date he downloads information. This may help him find it later in the site's archives.



- **Print out the data.** Online information is often here today and gone tomorrow, so paper copies are a must.
- **Be careful when using wikis.** Although Wikipedia (a well-known Internet encyclopedia) is generally reliable, other wikis may not be. If your child cites information from a wiki, he should verify it through other sources, too.
- **Be careful not to plagiarize.** Remind him that plagiarism is cheating and is a serious offense with serious consequences.

URL (Uniform Resource Locator): A website's address. Wiki: A site that allows users to add, edit or remove content.



What to Do If You Think Your Child is in Danger

- f you believe your child is in real danger from someone she's encountered online, you must act quickly. Here's what to do:
- If it's a dire situation (for example, she's left home to meet a stranger), call 911.
- If it's less urgent, notify your local police department. Contact the school if appropriate—signs of cheating, cyberbullying, potential drug trafficking, potential violence, etc.
- **Take a hard look** at your child's Internet use. You may want to change (or delete) her IM screen name and any online profiles.



Take a Pledge

Commit to staying safe and responsible online! Together with your child, review and sign this pledge. Post it near your computer.

- **1.** I promise NOT to post personal information— like my full name or address— anywhere online.
- **2.** I promise to tell a parent IMMEDIATELY if I come across anything scary or threatening online.
- **3.** I promise NOT to post photos of myself or my family and friends online.
- **4.** I promise to CLOSE the browser right away if I see pornography.
- **5.** I promise NEVER to respond to mean or threatening messages.
- **6.** I promise NEVER to set up a face-to-face meeting with someone I meet online unless a parent approves it.

Child	Date
Parent	Date

Resources

The Parent Institute maintains a list of current resources to help you guide your child toward safe and responsible use of the Internet.

- Tools that Can Help http://www.parent-institute.com/internetsafety/tools.pdf
- Know the Shorthand http://www.parent-institute.com/internetsafety/shorthand.pdf
- Glossary of Internet Terms
 http://www.parent-institute.com/internetsafety/glossary.pdf

Answers to the quiz: 1-a Your child is less likely to visit inappropriate sites if the computer is kept out in the open. **2-c** When it comes to Internet safety, there's no substitute for supervising your child's usage and letting her know what she's allowed to do online. 3-bWhile kids' chat rooms are better monitored than many adult chats, no chat room is "completely safe." 4-bThis screen name reveals the user's first name, hometown and birth year, all of which could be used to track her down. 5-c A study published in Online Victimization: A Report on the Nation's Youth showed that one child out of five was sexually solicited online over the course of a year.



Remember—you're the adult and you're in charge! You are the one with years of life experience. It is your responsibility to monitor your child's use of the Internet. It's not just a good idea—it is your responsibility!



Internet Safety & Responsibility for Students is published by The Parent Institute*, P.O Box 7474, Fairfax Station, VA 22039-7474. Call (800) 756-5525.

English Stock # 314A, Spanish Stock # 414A Copyright © 2009, 2006 The Parent Institute*, a division of NIS, Inc.

Publisher: John H. Wherry, Ed.D. Writer: Holly Smith. Managing Editor: Pat Hodgdon.
Staff Editors: Erika Beasley, Amanda Blyth, Jennifer McGovern & Rebecca Miyares.
Editorial Assistant: Pat Carter. Marketing Director: Laura Bono. Marketing Assistants: Joyce Ghen & Jennifer Hester. Business Manager: Merissa Larson. Translation Manager: Michelle Beal-García.
Customer Service Manager: Peggy Costello. Customer Service Associates: Louise Lawrence, Cynthia Lees & Margie Supervielle. Business Assistant: Donna Ross. Circulation Associates: Marsha Phillips & Diane Perry. Graphic Design and Illustrations: Joe Mignella, Maher & Mignella, Cherry Hill, NJ. Visit our website! www.parent-institute.com