The Internet is an extraordinary resource that links our children to a world of information, experiences and ideas that might otherwise be unavailable to them. However, the Internet can also expose our children to numerous risks, and it is crucial to remember that when a child is online, his or her safety may also be on the line. Just as you have taught your child basic safety rules for the physical world, you should also teach your child basic safety rules for the virtual world.

The following basic safety rules pertain to all types of Internet applications. Please review the rest of this pamphlet for more detailed information about different types of applications.

Basic Safety Rules

- Place your child's computer in an area where you are best able to monitor his or her online activities.
- Take an active interest in your child's online activities.
- Warn your child never to reveal *any* identifying information such as: last name, ethnicity, age, address, phone number, school name, parents' names, parents' employers or work addresses. *Caution your child that predators and con artists are experts at accumulating incremental amounts of personal data until they eventually obtain enough information to locate a user.*
- Warn your child that identity is easily concealed online and that people may not be who they claim to be. Explain to your child that, for example, an online "friend" who claims to be the same age as your child may in fact be an adult in search of a child victim.
- Warn your child **never** to arrange an in-person meeting with someone met online.
- Warn your child never to accept anything sent to him or her by a person met online.
- Warn your child never to post online a photo of any family member without your permission. Explain that online images may be altered or "morphed" and used on, for example, pornographic sites.
- Consider using filtering or blocking software. There is an extensive array of filtering and blocking software available. Some of it is free of charge. However, you should be aware that the software may not be completely effective; children may be able to bypass the restrictions, or your child may use a computer that is not equipped with these protective devices. See the resource section of this pamphlet to obtain more information on parental control devices.

E-Mail

E-mail (electronic mail) is a way of sending messages electronically from one computer to another, generally through a modem and telephone line connected to a computer. Children may have access to an e-mail account through your internet service provider, a school-based network, or an online service offering (sometimes free) e-mail accounts.

Potential Dangers

- Your child may reveal personal information to a dangerous stranger, such as a sexual predator or con artist.
- Your child may respond to e-mail from an unknown sender, thereby revealing his or her e-mail address to someone who should not have it.
- Your child may receive harassing or threatening e-mail.
- Your child may receive unsolicited e-mail ("spam") which contains sexually explicit material or junk advertisements.
- Your child may use e-mail to commit a crime, such as using e-mail to send threatening or harassing messages, disseminate child pornography, engage in drug dealing or gambling, or make purchases on items (such as firearms) not permitted by minors.

Precautions

- Unless you feel confident that your child will use e-mail safely, you should consider sharing an e-mail account with your child, having his or her e-mail routed through your account, or knowing your child's password. *However, even a relatively unsophisticated user may be able to bypass this attempt at supervision by establishing (free) e-mail account(s) with an online service. Therefore, it is imperative that you discuss safety issues directly with your child.*
- Warn your child not to respond to e-mail if the sender is unknown.
- Warn your child not to respond to angry or threatening e-mail.
- Warn your child not to share his or her password with anyone.
- Warn your child not to open or download any attachments in an e-mail sent by an unknown sender. The material may contain pornographic or other offensive material or a computer virus.
- Follow the general safety principles contained in this brochure.

Chat Rooms

A chat room is an online service that allows multiple users to communicate with each other about an agreed-upon topic in "real time."

Potential Dangers

- Your child may encounter someone who targets him or her for victimization.
- Your child may encounter a predator who is searching online for victims.
- Your child may encounter offensive language and adult content.
- Your child may commit a crime, such as transmitting a threat of violence.

Precautions

- Advise your child not to enter a chat room without your consent. *This advice will be most effective with younger children.*
- Remind your child that visitors to chat rooms often disguise their identity.
- Warn your child that a child predator may enter a chat room and "lurk"; that is, observe conversations but not participate. The predator may target a particular child without even participating in the conversation.
- Warn your child to avoid using either his or her real name or a provocative screen name.
- Instruct your child not to complete *any* online profile, as the profile could aid a sexual predator in locating a victim. An online profile may not be as anonymous as your child believes.
- Warn your child about the three most common questions pedophiles ask: 1) Are you home alone? 2) Who uses the computer? 3) Where is the computer? Tell your child not to respond to these questions and to leave the chat room immediately.
- Warn your child never to "go private" into a chat room with a stranger. Many chat programs allow for a private method of chatting. A predator may seek to go private with a child he or she is targeting for victimization.
- Warn your child never to accept any files sent by someone met online.
- Follow the general safety principles contained in this brochure.

World Wide Web

The World Wide Web (abbreviated as "www") consists of "pages" of information available on the Internet. These pages may be accessed either by searching for a specific address called a "URL" (for example, many retail businesses now advertise their online addresses) or using a search engine to search the Web by keywords or topics. Many Web pages contain "links" which allow the user to connect instantly to related Web pages.

Potential Dangers

- Your child may accidentally or intentionally enter a pornographic site containing adult or child pornography or a site which promotes violence, hatred, bigotry, drug use or other harmful behaviors.
- Since anyone may post material on the Web, some sites will promote false or misleading information masquerading as fact.
- Your child may be deceived into giving out personal information by falling for a crafty marketing scheme, such as an innocuous sounding survey or a contest.
- Your child may be exposed to marketing of drugs and/or alcohol which is geared toward children as there are no restrictions on such advertising methods on the Internet.
- Your child may download games which are excessively violent and/or promote hatred.
- Your child may use the Web to commit a crime, such as using information learned from the Web to build illegal incendiary devices,

to purchase illegal weapons or substances, to utilize illegal tools available on hacker sites, and to use propaganda found online to engage in hate crimes.

Precautions

- Advise your child to use the "back" key whenever he or she encounters a site which causes discomfort or fear. If that does not immediately return the child to the preceding Web page, your child should close all windows or quit out of the browser.
- Report any site containing child pornography directly to the Center for Missing and Exploited Children (www.missingkids.org; telephone 1-800-THELOST). *Be aware that the act of downloading child pornography is a felony under Massachusetts law.*
- Discuss the difference between reliable and unreliable sources of information with your child.
- Advise your child not to participate in any online surveys or contests or make any online purchases without your permission. Even if you are sure that a Web site is legitimate, you should check the posted privacy policy of a Web site before transmitting any personal information.
- Ask your child to review with you (using the "history" folder in your browser) the Web sites that he or she has visited. If your child is reluctant to have you review these sites, this may be a warning sign that inappropriate sites have been visited.
- Follow the general safety principles contained in this brochure.

Resources

For more information on the subjects discussed in this pamphlet, please visit your local library or contact the following organizations and sites:

The **National Association of Attorneys General** and the **Federal Trade Commission** have jointly produced a guide entitled, *Site Seeing on the Internet: The Savvy Traveler*, available at www.ftc.gov/bcp/conline/pubs/online/sitesee

The Children's Partnership
tel.: 202-362-5902 fax: 202-362-3598
www.childrenspartnership.org
This site contains the full text of its guide: *The Parents' Guide to the Information Superhighway: Rules and Tools for Families Online.*

America Links Up: A Kids Online Teach-In About Internet Safety
www.netparents.org
This site is sponsored by a broad coalition of educators, non-profit organizations, and corporations.

National Center for Missing and Exploited Children
HOTLINE: 800-843-5678
www.missingkids.com or www.ncmec.org

www.smartparent.com *and* **www.safekids.com**
These sites include detailed information about blocking and filtering software.

This pamphlet is available online at the Web site of the Office of Massachusetts Attorney General Tom Reilly, ***www.ago.state.ma.us.***

Warning Signs That Your Child May Be In Danger

It is normal for children, especially teenagers, to place a high value on their privacy. However, parents should be aware that unusually covert behavior on the part of a child may be an indicator of inappropriate Internet use. Other potential warning signs include:

- Your child has withdrawn from normal interaction with family and friends to spend an inordinate amount of time engaged in Internet activity;
- Your child turns the computer off or quickly changes the monitor's screen when you enter the room;
- Your child demonstrates a marked change in behavior, beliefs or attitudes;
- Your child's academic performance decreases significantly;
- You find pornographic, racist, or drug-related material on the computer;
- Your child is using multiple online accounts (including free e-mail services) or the online accounts of others;
- Your child is making or receiving unexplained long-distance calls;
- Your child has made unexplained, unauthorized use of a credit card while online.

The appropriate response will depend on the level of your concern. If you believe your child's safety is in danger, you should immediately contact your local police department. You should also contact your local police if:

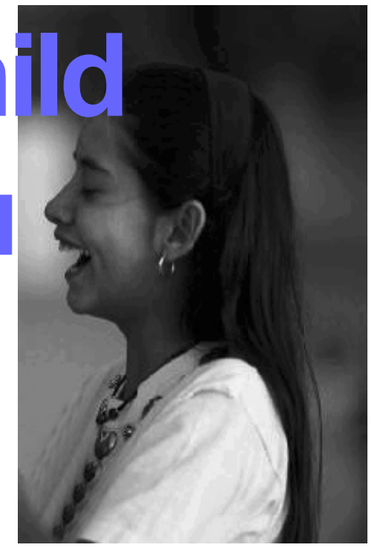
- Your child has received child pornography;
- Your child has been sexually solicited by someone who knows or should know that he or she is a minor;
- Your child has received sexually explicit images from someone who knows or should know that he or she is a minor;
- Your child or anyone in the household has been threatened.

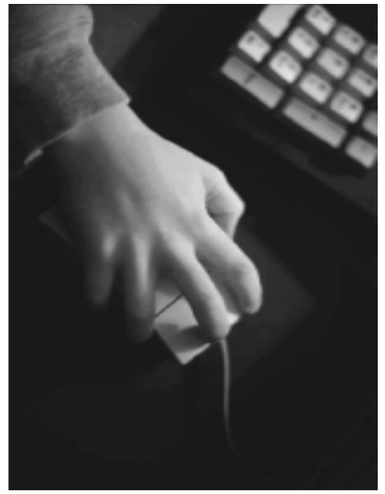
If you are concerned that your child's mental, physical, or social development is being adversely impacted by his or her online activities, you should seek professional assistance. School guidance counselors or your child's pediatrician may be useful sources of assistance.

Privacy and the Internet

The focus of this pamphlet has been on the potential risks posed by your child's use of the Internet. However, parents must also be vigilant in striving to prevent personal information about children (e.g., photographs, lists of enrollees) from appearing on the Web pages of schools, camps, and organizations that run or sponsor programs for children. When you enroll your child in a program, ask if there is a Web site and visit it. Ask to review any existing privacy policy. If you are concerned about the types of information accessible to the public, you currently have numerous options available, including: (a) withdrawing or not enrolling your child, (b) seeking the development of a privacy policy or a modification of an existing policy, or (c) requesting that information about your child be excluded from any publicly shared information.

The Internet, Your Child and You





What Every Parent Should Know

Dear Parent,

This guide was written to explain basic safety measures you can take to ensure that your child's experiences on the Internet are safe, productive and fun. The single most important thing you can do to keep your child safe is to talk with him or her. Explain what dangers exist and set clear ground rules. Revisit your rules and modify them, if appropriate, as your child becomes older. Encourage your child to talk about his or her experiences. If you are concerned about possible inappropriate use of the Internet, discuss these concerns with your child. The more you know, the safer your child will be.

Office of
Attorney General Tom Reilly

www.ago.state.ma.us