



VISION

The Pennsylvania Commission on Crime and Delinquency strives to be a state and national leader by providing innovative services and programs that promote justice for all citizens and communities of Pennsylvania.

MISSION

The Pennsylvania Commission on Crime and Delinquency promotes a collaborative approach to enhance the quality of justice through guidance, leadership and resources by empowering citizens and communities and influencing state policy.

VALUES

Commitment
Dedication
Respect
Integrity
Optimism
Teamwork

The Benefits of the Information Superhighway

The World Wide Web connects millions of people around the globe with an instant means of communication and a powerful tool for information gathering. The resources available on the Internet are constantly growing.

Reference information such as news, weather, sports, stock quotes, movie reviews, encyclopedias and airline fares are readily available online.

Users can conduct transactions such as trading stocks, making travel reservations, banking and shopping online.

Millions of people communicate through electronic mail (e-mail) with family and friends around the world.

Others use the public message boards to make new

friends who

share common interests.

With this educational and entertainment tool, users can learn about virtually any topic, take college courses, or play an endless number of computer games with other users or against the computer itself.

User “computing” is enhanced by accessing online thousands of shareware and free public domain software titles.

Most people who use online services have positive experiences. But, like any endeavor—traveling, cooking or attending school—there are some risks. The online

world, like the rest of society, is made up of a wide array of people. Most are decent, law abiding, and respectful, but some may be rude, obnoxious, insulting or even mean and exploitative.

Children and teenagers benefit from being online, but they also can be targets of crime and exploitation in this as in any other environment. Trusting, curious and anxious to explore this new world and the relationships it brings, children and teenagers need parental supervision and common-sense advice on how to be sure that their experiences in “cyberspace” are happy, healthy and productive.

***Some call it
Cyberspace,
others call it the
Information
Superhighway-
by any name,
it is still the
Internet.***



Putting Cyber Crimes in Perspective

Although there have been some highly publicized cases of abuse involving computers, reported cases are relatively infrequent. Of course, like most crimes against children, many cases go unreported, especially if the child is engaged in an activity that he or she does not want to discuss with a parent. The fact that crimes are being committed online, however, is not a reason to avoid using these services. To tell children to stop using these services would be like telling them to forego attending college because students are sometimes victimized on campus.

A better strategy would be for children to learn how to be “cyber smart” in order to better safeguard themselves in any potentially dangerous situation.

Guidelines for Parents

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

- ✓ Never give out identifying information i.e., home address, school name or telephone number;
- ✓ Get to know the services your child uses. If you don’t know how to log on, ask your child to show you;
- ✓ In every instance, no meeting should be arranged between your child and another Internet user without a parent accompanying your child;
- ✓ Never respond to messages or bulletin board items that are suggestive, obscene, belligerent, threatening or make you feel uncomfortable;
- ✓ Should you become aware of the transmission, use or viewing of child pornography while online, immediately report this to the National Center for Missing and Exploited Children by calling 1-800-843-5678. You also should notify your online service and your local police department;
- ✓ Remember that people online may not be who they seem to be;
- ✓ Remember that everything you see online may not be true;
- ✓ Set reasonable rules and guidelines for computer use by your children. Discuss these rules and post them near the computer as a reminder; and
- ✓ 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.

Children can learn to be “cyber smart” to safeguard themselves.



What are the Risks?

While there are risks for all children using the Internet, teenagers particularly are vulnerable because they are more likely than younger children to participate in online discussions regarding companionship, relationships or sexual activity.

How Children Find Questionable Things on the Internet:

There are a number of ways in which children find objectionable material online. Some children find questionable sites through search engines. “Search engines” are popular tools which may be accessed via highly-publicized web sites. Users can use the search engines to scour the Internet based on words or phrases. A search on “sex,” for example, may yield scientific information on human sexuality as well as a laundry list of pornographic sites. Search engines are a valuable Internet tool, but they can also be easily used by children to find inappropriate material.

Some may find a site by following links on other sites or by typing blind URL’s in the location bar of their web browser. A child does not necessarily have to be looking for anything particular to stumble onto a questionable site.



Children may also stumble upon inappropriate sites quite by accident, due to unscrupulous manipulation by some web site operators. If your child runs a search and the word "girls" is in the topic, nearly 17% of the web pages listed will be pornographic. If the word "boys" is in the topic, 15% of the results will be pornographic.

There are a lot of harmless words that can lead to x-rated websites. So watch out. Unsolicited x-rated email is another way our children can accidentally be exposed to pornography. These messages usually have innocent subject lines like, "yesterdays mail." Your child has no way of knowing that they are about to open a message containing seedy stuff. The best way to deal with this problem is to train your children to always click "back" or "home" on the web browser tool bar the minute they see an adult site or something inappropriate then, make sure they tell you.

Search Engines:

A "search engine" is a device or means a computer program uses to look for information on the Internet, relying on keywords or phrases provided by you. This engine, using the keywords you give it, searches pages, menus and files on the World Wide Web sites, Gopher sites, FTP sites, listservers and newsgroups. Searching the WWW requires a browser and basically requires you to use words and phrases in a certain way so that the "engine" will know exactly what you mean. If a search engine has other word/phrase locating techniques, a "help" link will be presented to assist you in your search.

Chat rooms:

Most Internet chatters do not use their real names. This allows for a significant degree of anonymity during chats. Thus, a teen in a chat room may think he is talking to another young person, when in fact he is holding a conversation with a predatory adult.

Most chat rooms offer users the ability to enter into private, by-invitation-only conversations. Sexual predators are well aware of this fact, and typically will try to lure a potential victim into private conversation. If the predator hopes to build a relationship or arrange a face-to-face meeting with a victim, it will generally be proposed during a private chat session.

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

Finding Chat Rooms:

Chats can be found on service providers' sites, through instant messaging systems like ICQ (I seek you) and AOL (America Online), and on the IRC (Internet Relay Chat). ICQ is a free software program that links individuals around the world. People can search for and contact others with similar interests. ICQ users identify geographic regions, hobbies, special interests and a whole array of personal information about themselves in their profile. AOL Instant messaging is similar to ICQ. The IRC is usually used by a well-informed Internet user, but this does not mean it is hard to access. The IRC is not moderated by a company like AOL, so it is a bit more dangerous for children. The IRC does not have a filtering process or a major service provider watching activity.

The following are some examples of where chat rooms can be found:

- Internet Relay Chat (IRC)
- Netscape Instant Messenger
- The Microsoft Network
- CompuServe
- ICQ (I seek you)

Chat room screen:

Chat room screens typically list the “screen names” of everyone in the room. Users who are logged onto the chat room may notice a message that certain users are entering and leaving the chat at various times. Messages typed by those in the chat room will be visible to all in the main screen area. A blank space for entering messages will be visible on the page.



Users may selectively filter out messages from other users they find annoying. Alternately, they may choose to be alerted when friends enter or leave the room.

From time to time, an instant message may pop up onscreen. This is a one-on-one message from another user. The recipient may choose to reply or ignore the instant message.

Bulletin Boards and Newsgroups:

Bulletin boards and Usenet newsgroups are places on the Internet that people can access and leave messages for anyone to read. Anyone can visit public sites and read or view any “posted” message or picture.

Files of all sorts can be attached to messages and left on a newsgroup. Users who visit later can download the file if they choose.

Most Usenet newsgroups are unregulated. Topics range from positive activities and discussions to fringe and even illegal activities.

The major web browsers will enable the user to scan Usenet newsgroups, as will specialized “reader” software.

Bulletin boards, or discussion forums, generally are attached to web sites and are regulated to some extent. The concept is similar in that users post messages. Others can reply or post a message of their own.

Gangs in Cyberspace:

The gangs that exist on the Internet include the same gangs that walk our nation’s streets. Many gangs in the United States have a presence on the Internet including: motorcycle gangs, street gangs, drug gangs and hate gangs like the KKK (Ku Klux Klan).



Online Stalking and Harassment:

Online stalking occurs when one Internet user follows another to various locations in cyberspace or by sending repeated, unwanted messages. An additional type of harassment occurs when a user poses as

another to post false, often inflammatory messages via e-mail, newsgroups or online message forums.



Stalkers use tools such as the AOL “Buddy List” to locate and track the movements of their victims. Additional tools built into programs such as Internet Relay Chat (IRC) allow stalkers to find the locations of victims when they are online.

Additionally, stalkers may use a variety of online resources in an attempt to find a potential victim's address, phone number or other personal information.

Information to Protect Your Children

What Parents Need to Do!

1. It is important that parents take the time to learn how to use the family computer and the Internet. This must be viewed as an investment in the child's safety. A parent whose Internet awareness lags behind cannot properly monitor the child's online activity.
2. It is essential that parents discuss the online environment with their children. Fostering this type of communication will help parents grasp where their children are visiting online, and with whom they are communicating.
3. Parents are encouraged to discuss the Internet in positive terms with their children. It is more productive to share good sites that will pique a child's interest than to stress the negative destinations.
4. It is important that a parent devote some time to watching their children online. Experts advise that the computer be placed in a common room.
5. Parents should have a working knowledge of how to check the family computer to find out where their children have been. Internet activity leaves a trail that is easily checked.
6. As with other activities in life, at times it is a parent's responsibility to say "no" when a child requests to participate in a certain activity online. For example, some parents may not be comfortable with their children visiting chat rooms or downloading a certain game.
7. It is important to develop a set of family rules for computer usage. Parents should discuss these with the child and explain why they are needed.

Key Points to Remember:

- Understand the technology;
- Watch children while they are online;
- Listen and talk to them when they are off-line;
- Know how to check where they have been;
- Sometimes you have to say NO; and
Create a set of rules.

Filtering Software:

Filtering software products can be installed on a computer to both limit and monitor computer and Internet use.

Such products can block access to objectionable sites. In addition, they will log where the computer has visited, often in a way that is more “user friendly” than extracting the same information from a web browser.

Some products can be set up to block the release of personal information, such as phone and credit card numbers. Parents can typically customize the products to suit their concerns.

Filtering software is not a perfect solution. It often inadvertently blocks access to positive sites. In addition, it raises issues of privacy and trust, especially with older children. Finally, the “filters” often need to be updated, creating a time lag in which newer inappropriate sites are not screened.

Such software can be beneficial, but parents must understand both its uses and limitations. The key point is that even the best filtering software is no substitute for parental involvement in a child’s Internet use.

There are several software companies that sell filtering or blocking software. Some allow for a limited time, free download of their product to allow parents time to evaluate the program. Many organizations support the family with providing a safe and enjoyable Internet experience. Some of the software or rating organizations systems use the controls provided in web browsers.

Software that is available to filter World Wide Web sites on your home computer include:

- Kidsproof Cyberpatrol
- Cybersitter Surfwatch
- Netnanny Cyber Sentinel Internet Filter

Organizations that can assist you in filtering World Wide Web sites on your home computer include:

- RSACi <http://www.icra.org/>
- Safe Surf <http://www.safesurf.com/>

AOL Parental Controls:

America Online (AOL), is the largest Internet service provider in the world. Because of America Online’s enormous subscriber base, it is likely that many parents who attend Internet Safety training will be AOL users. For that reason, a section is included on AOL’s parental controls.

These controls, which can be accessed by AOL keyword “parental controls,” offer options which are both useful and powerful. These parental controls allow parents to designate different levels of access for each child. Control categories include “Kids Only” for children under 12; “Young Teen” for ages 13-15; “Mature Teen” for ages 16-17 and 18+. Parents can configure the controls to block Instant Messages, chat, private chat, or downloading of files. In addition, parents may restrict their children’s e-mail or block files attached to e-mail. A “Buddy List” feature may be used to set up a safe list of AOL friends. Inappropriate web sites can also be reported via the controls.

How to Check Where My Child has Visited on the Internet?

Web Browsers Tell All:

At present, Netscape Navigator and Microsoft Internet Explorer are by far the most popular choices for web browser software. Fortunately for parents, both leave “trails” which can be examined to determine which web sites the user has visited.

Netscape URL History:

- Keystroke Control H pops up the history of URLs the browser has visited. The number of days contained in the history file is identified and can be changed by selecting Preferences on the Edit option.
or,
- To view the History, click “Communicator,” then “Tools,” then “History.”
or,
- Click the drop-down arrow at the right side of the Address Bar. This will reveal a listing of web sites visited. In Netscape, users often store their preferred web sites as “Bookmarks.” This grouping can be accessed from the Internet Explorer screen by clicking on “Bookmarks” along the tool bar. To view contents of folders stored within Bookmarks, simply scroll the mouse down until the folder is highlighted.
- Users often select a favored web site as their “start page.” This will be the page that the browser opens to whenever the user goes online. Simply starting the browser will reveal this page.

Microsoft Internet Explorer History:

- To view pages visited in previous sessions, click the History icon on the toolbar (looks like a sun dial), and then click the appropriate folder. Alternatively, click “View,” then “Explorer Bar,” then “History.” In newer versions you can also use “Control H.”

or,

- Click the drop-down arrow at the right side of the Address Bar. This will reveal a listing of web sites visited.
- “Cookies” are small files which save information about web sites on the user’s hard drive. Cookies often include things like web site passwords. To check cookies, examine the contents of the folder
C:\windows\temporary Internet files.

Glossary of Terms

Commonly Used Acronyms and What they Mean

Internet communication is filled with acronyms, frequently used phrases condensed to two or more letters. Learning these acronyms will help you understand what others are saying. The following are some of the most common acronyms:

AFAIK as far as I know

AFK away from keyboard

BBIAF be back in a few

BBL be back later

BRB be right back

BTW by the way

FAQ frequently asked questions

IMO in my opinion

IMNSHO in my not so humble opinion

IMHO in my humble opinion

IRC Internet Relay Chat

LOL laughing out loud

RENTS parents

ROTFL rolling on the floor laughing

LTNS long time no see

RE regards, or re hi, or hi again

OTOH on the other hand

RTM read the manual

TTFN ta ta for now

WB welcome back

IRL in real life

Emoticons

Also known as a “smiley,” this is a combination of characters that suggests an emotion when read sideways. Examples include:

- :-) Smiling face to express humor
- :) Smiling face without a nose; variation of above
- :(or :- (Frowning face to convey sadness or displeasure
- ;-) Winking smiling face used to convey humor or flirtation
- 8-) Wide-eyed smile used to show shocked pleasure
- :-p Face with tongue stuck out
- :-p~ Face making a “raspberry”
- :-o A look of shock

Internet Lingo/Select Terms

BBS (Bulletin Board System)

- Areas within the Internet where you can post messages and announcements.

Bot (Short for infobot or knowbot)

- A program used to search the Internet for data.

Browser

- A browser is a software program that allows you to connect with the World Wide Web (WWW) (provided you have an Internet connection) and view the contents of web sites. Netscape Navigator and Microsoft Internet Explorer are currently two popular browsers.

Cyberspace

- The total range of information available through computer networks. A term coined by author William Gibson in his book *Cyberpunk*.

E-mail

- Messages sent between computers with an Internet address.

FAQ (Frequently Asked Questions)

- Canned answers to questions everyone asks.

Freeware

- Software which can be used without any payment, generally downloaded from the Internet.

FTP (File Transfer Protocol)

- A method of transferring files to and from remote computers. The code that allows users to transfer files from one computer to another over phone lines. Pages transferred to a web site use FTP.

GIF (Graphics Interchange Format)

- A visual image file format.

Gopher

- A menu-based method of searching for information on the Internet.

Home page

- The first screen you see when you enter a web site. The Home page first appears when you enter a URL and “go to” that site. Home pages usually contain general information about the site and have links to the other pages on the site.

Hyperlink

- An object (text or graphic) containing a link to a web page. When you click on a hyperlinked object, you are automatically connected with another web page. It may be another page on the same site, or it may be a page on a different web site.

HTML (HyperText Markup Language)

- The rules that govern the way documents are created so that can be read by a WWW Browser.

HTTP (HyperText Transport Protocol)

- The standard for moving hypertext files across the Internet.

IRC (Internet Relay Chat)

- A computerized way for people to congregate and chat together.

JPEG (Joint Photographic Expert Group)

- A visual image file format.

MIME (Multiple Internet Mail Extensions)

- Things you can include with e-mail, sent over the Internet i.e., audio, visual images, text messages.

Modem

- A modem is a device that connects your computer to other computers via a phone line. The contraction means MODulate DEModulate.

MPEG (Moving Pictures Experts Group)

- A method for storing movie files.

Netscape Navigator

- A browser for accessing the World Wide Web.

POP (Point of Presence)

- An Internet access node of an Internet service provider or the number your modem rings to get online.

POP3 (Post Office Protocol 3)

- A type of e-mail system which stores messages on your service provider's machine and downloads them automatically when you are online.

PPP (Point to Point Protocol)

- A regular phone line that connects to the Internet.

Shareware

- Software which can be used for free for a trial period, after which a small payment is expected. Shareware is generally downloaded from the Internet.

SMTP (Simple Mail Transfer Protocol)

- A type of electronic mail protocol which governs the format of e-mail messages.

Site

- Short for web site. This is a page or group of pages containing text and graphics that can be accessed by anyone with an Internet connection.

Spam

- An unprofessional slang term referring to sending a message to multiple newsgroups, mailing lists or individuals that did not ask for it.

TCP/IP (Transmission Control Protocol/Internet Protocol)

- The communications protocol that connects your computer to the Internet.

Telnet

- The command program used to access other servers on the Internet.

URL (Uniform Resource Locator)

- Indicates the address of a specific source of information, usually a web site. A URL is the string of characters you type into browsers to reach a certain web site. For example, <http://www.pccd.state.us> is the URL for the Pennsylvania Commission on Crime and Delinquency web site.

WWW (World Wide Web)

- A hypertext based system that allows you to retrieve information from around the globe. A part of the Internet that allows users to view documents containing text, graphics and hyperlinked objects.

CyberTipline - 1-800-843-5678

The National Center for Missing and Exploited Children, in partnership with the Federal Bureau of Investigation, U.S. Customs Service and the U.S. Postal Inspection Service, serves as the national CyberTipline and as the National Child Pornography Tipline 1-800-843-5678.

The CyberTipline handles leads from individuals reporting the sexual exploitation of children including: possession, manufacture, and distribution of child pornography; online enticement of children for sexual acts; child prostitution; child-sex tourism and child sexual molestation (not in the family).

If you know about a child who is in immediate risk or danger, call your local police.

If you have any information on a missing child, call **1-800-THE-LOST**.

Contact CyberTipline if you have information that will help in the fight against child sexual exploitation. Your information will be forwarded to law enforcement for investigation and review and, when appropriate, to the ISP.

Keep this pledge at your computer.

My Rules for Online Safety:

- ✓ I will not give out personal information i.e., my address, telephone number, parents' work addresses or telephone numbers, or the name and location of my school without my parents' permission.
- ✓ I will tell my parents immediately if I come across any information that makes me feel uncomfortable.
- ✓ I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring one of my parents along.
- ✓ I will never send a person my picture or anything else without first checking with my parents.
- ✓ I will not respond to any messages that are mean or make me feel uncomfortable. If I do, I will tell my parents immediately so that they can contact the online service.
- ✓ I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that 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.

*Courtesy of The National Center for
Missing and Exploited Children*

**Cyber Tipline:
1-800-843-5678**

USEFUL SITES

- **Pennsylvania Commission on Crime and Delinquency**
www.pccd.state.pa.us
- **Pennsylvania State Police**
www.psp.state.pa.us
- **Center for Schools and Communities**
www.center-school.org
- **National Center for Missing and Exploited Children**
www.missingkids.org
- **National Crime Prevention Council**
www.ncpc.org

CREDITS

- **Pennsylvania Office of Juvenile Justice and Delinquency Prevention / Law Enforcement Workgroup**
- **Pennsylvania State Police**
- **Abington Township Police Department**
- **Bellevue Borough Police Department**
- **Cranberry Township Police Department**
- **Pennsylvania Commission on Crime and Delinquency**
- **Center for Schools and Communities**
- **The Pennsylvania Department of Education**

Available through our video lending library is an accompanying video entitled “Cyber ‘Rent.” For more information on obtaining this video please call toll-free 1-877-R-PA-KIDS, Ext. 3102.

The Pennsylvania Commission on Crime and Delinquency offers a training curriculum on Internet Safety.

If you or your group are interested in attending an Internet Safety Training Program please contact staff at the PCCD, toll-free, at 1-877-R-PA-KIDS, Ext. 3102, or visit our website at www.pccd.state.pa.us to identify the location of the next scheduled internet safety training curriculum that will be offered in your area.



Pennsylvania Commission on Crime and Delinquency

Edward G. Rendell, Governor

3101 North Front Street, P.O. Box 1167, Harrisburg, PA 17108-1167
1-877-R-PA-KIDS, 1-717-705-0904, Fax: 1-717-705-3698, www.pccd.state.pa.us