

Safe Surfing



An Internet Safety Manual for
the Community of Easton, CT

Did You Know?

Thirty-three percent of 13-17 year-olds, and 48% of 16-17 year-olds report that their parents or guardians know “very little” or “nothing” about what they do on the Internet.

<http://www.theantidrug.com>

One of every 17 minors online has been threatened or harassed online.

<http://www.cyberangels.org/statistics.html>

An alarming 75% of children share personal information about themselves willingly over the Internet in exchange for goods and services.

<http://www.cyberangels.org/statistics.html>

One out of five U.S. teens who regularly “log on” to the Internet have received a sexual solicitation or a sexual approach over the Internet, one in 33 have been aggressively pursued sexually online.

<http://www.cyberangels.org/statistics.html>

Sixty-four percent of online teens say that most teens do things online that they would not want their parents to know.

<http://www.theantidrug.com>

Seventy-seven percent of youths are contacted by an online predator by age 14, and 22% of children ages 10 to 13 are approached online.

<http://www.cyberangels.org/statistics.html>

Only 25% of children will tell a parent about an encounter with a predator who approached or solicited sex while on the Internet, and less than 10% report sexual solicitation to legal authorities.

<http://www.cyberangels.org/statistics.html>

Only 1/3 of online households in the United States proactively protect their children and teens by using filtering or blocking software.

<http://www.cyberangels.org/statistics.html>

Cover design courtesy of Frank Pagliaro.

Safe Surfing

An Internet Safety Manual for
the Community of Easton, CT

This manual was produced by the Easton Operation Respect Internet Safety Committee in cooperation with Samuel Staples Elementary School and Helen Keller Middle School for the Community of Easton, and published by Easton Operation Respect and the Easton PTA.

Should any organization wish to adapt this manual for its own publication, permission is granted providing you cite our organization in the publication as follows: "This manual was produced using 'Safe Surfing: An Internet Safety Manual for the Community of Easton, CT,' produced primarily by the Easton Operation Respect Internet Safety Committee, as a model." Please send one copy of your manual to: Easton PTA Internet Safety Committee, c/o Helen Keller Middle School, 360 Sport Hill Road, Easton, CT 06612.

First printing 9/06

TABLE OF CONTENTS

Did You Know?	Inside Front Cover
Letter	3
Parent/Guardian and Child Internet Contract	5
Websites	7
Photo and Video Sharing Websites.....	11
Social Websites	14
Netiquette.....	17
Email	19
Instant Messaging (IM)	21
What are the Warning Signs that Your Child Might Be At Risk Online?	23
What Should You do if You Suspect Your Child Is Communicating with a Sexual Predator Online?	25
Identity Theft.....	26
Chat Abbreviations	28
Glossary	30
References.....	37
I Have the Right to Feel Safe on the Internet	Back Cover

Note: Terms appearing in ***bold italic*** type throughout the manual are contained in the Glossary.

I HAVE THE RIGHT TO FEEL SAFE ON THE INTERNET

I have the right to explore, learn, and enjoy all the good stuff on the Internet.

I have the right to keep all information about me a secret.

I have the right not to be bothered or bullied by others.

I have the right to ignore emails and messages from people I don't know or trust.

I HAVE THE RIGHT NOT TO FILL OUT FORMS OR ANSWER QUESTIONS I FIND ON THE INTERNET.

I have the right to ask for help from a parent or an adult.

I have the right to report anyone I think is acting weird, or asking weird questions.

I have the right not to feel guilty if inappropriate stuff shows up on my computer screen.

I have the right for people to show me respect on the Internet.

I have the right to feel safe and to be safe on the Internet.

Dear Members of the Easton Community,

It has never been more evident than today that it takes a village to raise a child. The world is changing at an alarming rate and the parent of today needs to become an expert at child rearing, education, politics, health and welfare issues, changing technology and so much more to stay up to speed. Though there might be some discussion around which advances are good and which are bad, there is no denying that it is a different world today than when we were children.

We recognize that it is overwhelming to keep up with all of the changing technologies used by our children. Attaining a comfort level regarding electronic devices is increasingly difficult as the hardware and software evolve seemingly instantly before our eyes. While offering connections and information, these devices, if unsupervised or misused, can be extremely harmful. With just a few clicks of a mouse, our children can be innocently lured into dangerous cyber “neighborhoods” where access to high risk interactions and sites is easily available.

The statistics on the inside front cover are shocking. As a community, we must all be informed of the risks facing our children and take steps to train and protect them. Just as we would not hand our children keys to the car and expect them to drive without proper training, we need to guide our children to surf the Internet safely.

This handbook provides information to help you understand the Internet and monitor a child’s use in the interest of safety. Maintaining on-going, open lines of communication and establishing ground rules are important steps in preventing tragedy resulting from improper Internet usage. We have included a contract that a family should discuss and sign. The contract represents a commitment to safe and respectful use of the Internet and should be modified to suit the needs of each family at different developmental levels. We must all learn that discussions regarding

appropriate and safe use of the Internet should occur often and as naturally as we remind our children to brush their teeth.

While not all encompassing, the goal of this handbook is to provide enough information to open the doors of conversation to a broad audience. It is not the answer to all technological concerns, but hopefully for our community, it is a place to start.

Safe Surfing to Everyone!

The Internet Safety Task Force Committee,

Dana Johnson, Chair

Members: Richard Colangelo, Arlene Darrow, Lynne Duffy,
Susan Kaster, Marie Mas, Tony Neidenbach, Jeanine Pagliaro,
Joan Parker, Officer Mark Pastor, Kim Ryan, Pat Thomas,
Carol Weinshel, and Joan Winter

PARENT/GUARDIAN AND CHILD INTERNET CONTRACT

I want to use the Internet and I know that there are certain rules about what I should do online. I agree to follow these rules, and my parents/guardians agree to help me follow these rules:

- I will not give my name, address, telephone number, school, or my parents' or guardians' names, addresses, or telephone numbers to anyone I meet on the computer.
- I will tell my parents/guardians about people I meet while online. I will also tell my parents/guardians before I answer any emails I get from new people I meet online. I understand that sometimes people online pretend to be someone else. Sometimes they pretend to be kids when they are really adults.
- I will not buy or order anything online without asking my parents/guardians, nor will I give out any credit card information.
- I will not fill out any form online that asks me for any information about my family or myself without asking my parents/guardians first.
- I will not get into arguments or fights online. If someone tries to start an argument or fight with me, I will not answer him or her and will tell my parents/guardians.
- I will click on the "back" button or log off the computer if I see something I do not like, or that my parents/guardians would not want me to see.
- I will tell my parents/guardians if I see people doing things or saying things to other kids online that I know they are not supposed to do or say.
- I will not keep online secrets from my parents/guardians.
- I will tell my parents/guardians if someone sends me any pictures, or links to sites I know I should not be going to, or any email or instant messaging using bad language.

- I will tell my parents/guardians if someone asks me to do something I am not supposed to do.
- I will not call anyone I meet online unless my parents/guardians say it is okay.
- I will never arrange a meeting in person, with anyone I meet online, unless my parents/guardians say it is okay.
- I will never send anything to anyone I meet online, unless my parents/guardians say it is okay.
- I will tell my parents/guardians if anyone I meet online sends me anything.
- I will not plagiarize and use something I find online and pretend it is mine.
- I will not say bad things about people online, and I will practice good Netiquette.
- I will not use bad language online.
- I know that my parents/guardians want to make sure I am safe online, and I will listen to them when they ask me not to do something.
- I will help teach my parents/guardians more about computers and the Internet.
- I will practice safe computing, and check for viruses whenever I borrow a disk from someone or download something from the Internet.

I will follow these rules whenever and wherever I am on the Internet, including at home, at a friend's house, at a relative's house, at school, at a library, or on a cell phone.

I promise to follow these rules.
(Signed by child/teen)

I promise to help my child follow these rules and not to overreact if my child tells me about bad things that happen in Cyberspace.
(Signed by parent/guardian)

WEBSITES

What is it?

A Website is a set of interconnected webpages on the *World Wide Web (www)* that are coded in *HTML* and linked to each other and often to pages on other websites. Websites usually include a beginning file called a homepage, which is the first document users see when they enter the site. A website is hosted on a server by its owner or at an *Internet Service Provider (ISP)*, an organization that provides access to the *Internet*. Each site is prepared and maintained as a collection of information by a person, group, or organization.

How is it used?

An Internet Service Provider (ISP) provides access to websites and other areas of the Internet. Access to the ISP is either through a modem, which connects the computer to a telephone line, a high-speed *broadband* connection, or cable *modem*. Newer cell phones may also come with a web *browser*.

There is a wide array of services and information available online. Users may make travel reservations, shop, or conduct research for homework assignments. There are millions of websites on just about every topic imaginable.

Safety Concerns

Predators

- While some websites are wonderful, others may contain “adult” content and images. The sites themselves may be demeaning, racist, sexist, or contain false information. It is possible for children to stumble across any of these sites when conducting a search through a “*search engine*” because search engines do not filter out material that might be inappropriate for children.
- Websites sometimes ask for personal information such as name, address, and *email* address before letting the user

onto the site. The hook may be to attract the user to provide information in exchange for a promotional item or contest entry. Websites can be deceiving; just because a site appears to be maintained by a trustworthy individual or organization, it may not be. Anyone can set up a website, so it is important to be extremely careful before releasing information.

- There are “adult” pornography sites and areas on the Internet that contain illegal child pornography. Some of these sites attempt to verify the user’s age and/or require the user to enter a credit card number on the presumption that children do not have access to credit cards. It is important to immediately report any such site to the National Center for Missing and Exploited Children’s CyberTipline® at www.cybertipline.com.
- Some children have their own websites or post information on sites maintained by friends or an organization. These “social” websites are where teens regularly post their cell phone numbers, school names, pictures of themselves and other personal information. *These sites do not shield minors from pornographic images and sexual predators.* By utilizing these sites, children are inadvertently putting themselves at a higher risk from offenders or from people with bad intentions.

Caution

- Caution should be taken when downloading anything from a website. Some websites ask permission to download a program. These programs are sometimes used to display advertising on the computer. They are also capable of causing considerable harm to your computer or information, including invading a user’s privacy by tracking what they are doing online. They can plant a *virus* or increase the risk of an attack by a *hacker*. Nothing should be downloaded unless there is certainty that the material is coming from a reliable source. There is software available to scan for viruses, but no software, however, will catch everything.

Filtering and Monitoring Options

- There are ways to filter what a child can see on the World Wide Web. Some online services and ISPs allow parents to limit their children's access to certain websites. They offer age-appropriate *parental controls*.
- There are software programs that block websites which are known to be inappropriate for children. Some programs have the capability of preventing children from providing personal information about themselves. Visit www.getnetwise.org/tools for a list of these filtering programs.
- Rating systems rely on website operators to indicate the nature of their material. Internet browsers can be configured so that children are only able to visit sites that are rated at the level that their parents have specified. The advantage to this approach is that only appropriately rated sites can be viewed. However, this approach may block appropriate websites that have not submitted themselves for a rating and will therefore be blocked.
- Monitoring tools have the ability to inform adults about a child's online activity. Some of these tools only record the addresses of Websites where a child has been. Others actually provide a warning message to the child when he/she visits an inappropriate site. Monitoring tools can be used with or without the child's knowledge. Visit <http://kids.getnetwise.org/tools/tool/result.php3> for a list of some of these tools.
- It is possible to view the browser "history" which shows each of the sites visited. Every browser has a different way of accessing this information. For example:

Internet Explorer

- **To view the *history*:**
Click on the history button on the top, or click on "View," "Explorer Bar," "History," or just press the "control key" and "h" key together.

- **To adjust the number of days kept in the history:**
Click on “View,” “Internet Options,” and then use the up or down arrow in the history section to adjust the number of days.

Netscape

- **To view the history:**
Click on “Communicator” then “History” (on some versions, it is Communicator >Tools >History) or just enter “control + h”
- **To adjust the number of days kept in the history:**
Use the above procedure; in the history window, click “Edit,” “Preferences” and enter the number of days.

For a different version browser or a different browser altogether, use the help option to find out if history is available and how to access it.

Be aware, however, that *a child can clear the history of sites visited*. If the history file has been emptied, find out why. Visit www.familyinternet.com for more details.

While technological child-protection tools are worth exploring, they are not a cure-all. No program is foolproof; there is a chance that something inappropriate could slip through, or that something appropriate will be blocked. Some programs do not control **Instant Messaging (IM)** or **chat** services while other filters may not work with **peer-to-peer networks** that allow people to exchange files such as music or pictures. These peer-to-peer networks are sometimes used to distribute pornography.

Filters are not a substitute for parental involvement. The best way for parents to ensure positive online experiences is to be fully aware of what their children are doing online. Locating a computer in a common area of your home, rather than in your child’s

bedroom, can help to ensure this. Remember, your child can also access the Internet from a friend's house, the library, or even from a cell phone.

There are many sites where Internet safety issues are addressed. Visit <http://www.usdoj.gov/criminal/cybercrime/links1.htm> for a list of these sites. The information and material attained through these links does not necessarily represent the position or opinions of the *Internet Safety Committee*; these sites have been provided solely as an educational resource.

PHOTO AND VIDEO SHARING WEBSITES

What Are They?

Photo and video sharing websites allow users (including children and teens) to upload their digital photos and add captions, ***Blog*** comments, notes and ***tags*** posted from anyone in the world who has Internet access. YouTube, Yahoo Video and Google Video are examples of video sharing sites. Homepages with ***Buddy Lists*** of screen names are a typical feature.

How Are They Used?

People use these types of websites to upload, download, store, search, share, organize photos and videos, and interact with anyone in the world who has Internet access. These websites are competing in one of the fastest-growing entertainment segments on the Web. The majority of videos depicts budding musicians, comedians, filmmakers, or people vying for attention in harmless, and sometimes odd-ball, ways.

How Do They Work?

Photo Sharing Websites - Users easily, and at no cost, can create their own website usually consisting of a homepage. You can then upload, store, manage, organize, and add comments to your individual photos, create tags or comments within areas of photos, maintain Buddy Lists, and purchase prints. You can also search and view others' photos or photo albums, download others' photos,

add comments to others' individual photos, and create tags or comments within areas of others' photos. These websites often require you to register and to download their software to your Personal Computer (PC).

Video Sharing Websites - Users easily, and at no cost, can create their own website, or profile. Then you can upload, tag, and share your videos worldwide. You can also search and view others' videos, download others' videos, join video online communities with similar interests, and integrate videos on other websites you may have (such as a MySpace or MSN Space). As with photo sharing sites, these video sharing websites also require you to register and to download their software to your PC.

Safety Concerns

One in five children will be solicited online in his/her lifetime. We have to help our children understand the risks involved with posting anything on the Internet. Our children must be made aware that over 90 million people have easy access to information posted on the Internet.

- Parents need to discuss with their children, the implications of posting images and information (no matter how insignificant the information seems) about themselves, or about other children on the Internet.
- Parents also need to stress the importance of **transparent Internet use**, especially when children are posting or uploading any type of material, including photos, text, comments or video.
- The features of these sites attract children to innocently submit personal information about themselves and their families.
- Children and teens upload their **digital** photos and add captions and comments. What seems fun and harmless (posting pictures from a party or sleepover with funny comments about you and your friends, or posting pictures about your sports team, or your school) can actually make it easy *for any Internet user in the world* to gather personal information about your child and his/her friends.

- Many of the companies that let users display homemade videos on the Web are having difficulty keeping their pages smut-free. Sadly, videos with sexual and violent themes are easily obtainable.
- Another aspect of these websites involves *Cyberbullying*. This typically happens when a child is being cruel to others by posting harmful photos or videos of other children, with or without derogatory comments. Posting photos and content that humiliate, embarrass, harass, threaten, disrespect, insult, intimidate or torment someone else is unacceptable behavior.
- The content (the images and comments) that is easily accessible within these websites is not adequately filtered or monitored and contains material for mature adults only.
- Video sharing websites present an even more hazardous situation for children. Again, people use these websites to express themselves. Live video with sound has a much greater emotional impact than still photos with text. Much of the content on these websites, that children and teens can access, contains material for mature adults only. These websites are not adequately filtered or adequately monitored for children. As with photo sharing websites, posting videos that humiliate, embarrass, harass, threaten, disrespect, insult, intimidate or torment someone else is unacceptable behavior.
- All parents should personally investigate as many of these websites as possible to understand firsthand the benefits and the dangers associated with children accessing and using these websites.
- Monitoring your child's online behavior is no different than monitoring your child's behavior in public and at home.

SOCIAL WEBSITES

What Are They?

Social websites, also known as Blogs or Online Communities, provide a venue for individuals to create a website with personal information, such as a profile, photos, audio and video. Social websites enable interaction with anyone—anywhere—who has Internet access. Some examples include: MySpace.com, Blogger, Classmates, Xanga, America OnLine (AOL), Microsoft (MSN), and Yahoo.

Social websites are actually “Social Network Services,” which utilize Social Software, and many Social Networks are also Blog hosting services. Social Software applications allow people to connect or collaborate through computer-mediated communication to form Online Communities, which combine one-to-one (Instant Messaging, email), one-to-many (Webpages, Blogs), and many-to-many (*Wikis*) communication tools and interaction tools.

Communication tools are typically “one way” and manage the capture, storage, and presentation of text, audio, and video communications. Interaction tools, which are “live” (phone, net phone, video chat), or “near live” (Instant Messaging, *text messaging*, chat), handle online interaction between two or more users, with the focus on establishing and maintaining a connection among users.

How Are They Used?

People use these venues to express themselves. These websites enable people to share personal information, files, pictures, audio and video with anyone in the world with Internet access. Users can share their creativity, communicate with others, and meet new friends. Some of these websites offer security features that provide semi-private to private access and interaction with others. Most offer little to no security features and individuals’ “space”/profile/information can be accessed by, and individuals can interact with, anyone in the world who has Internet access.

How Do They Work?

Users easily, and at no cost, create their own personal website usually consisting of a homepage/profile page, where they post pictures, audio and video. These free personalized websites provide instant messaging capability (with Buddy Lists), online chat and email. These capabilities are expanding into offering “*live*” *electronic communication* tools where users can communicate via audio and video calling, and file sharing between their PCs, landline phones, and mobile phones. *Chat rooms* and IM are becoming superseded by live voice, or streaming video and direct voice communication. These websites typically require you to register and to download their software to your PC.

Safety Concerns

Predators

- Children can become visible and accessible to anyone in the world who has Internet access. The information and images posted determines the vulnerability and risks of any child participating. Children innocently give out information online, and information about them can easily be found by strangers.
- The information and visual content accessible within these websites are not adequately filtered monitored and may contain material suitable for mature adults only. Everyone, children included, can easily access inappropriate content.
- Registration to these sites requires that you give personal information; your name, email address, zip code, gender, birthdate, state, country, maiden name, high school (and graduating class). Even though most of these websites have policies prohibiting children under 14 years old from registering, the reality is anyone can submit any age, and there is no verification process.
- Furthermore, anyone can assume a different identity other than their true identity, so you cannot be assured the person portrayed is the same person who has posted the images and information.

The new live voice, streaming video, and voice applications being added to these websites present new concerns, but may help to alleviate the anonymous aspects of text-based communication. We have all heard the stories of adults posing as children using text-based IM and Chat. If you have visual and voice recognition of the person with whom you are communicating, you can determine the approximate age, gender, etc. of that person. However, if visual and voice connections are made with a child by strangers or predators, new risks are introduced with a higher level of concern.

There are some new social websites for children under 12 years old and families that have safety features such as user authentication (via credit cards), parental monitoring tools, and security features for a monthly fee.

Bullying

- The opportunity for Cyberbullying on social websites is great.
- Cyberbullying is being cruel to others by sending or posting harmful material.
- To children, posting materials on the Internet can seem impersonal so it is very easy for them to post harmful material.

Caution

- When children create personal spaces, profiles, or personal websites without informing their parents, they expose themselves to everyone in the world who has Internet access. This can create a very dangerous situation for your child and the whole family.
- Parents should personally investigate as many of these websites as possible to understand firsthand the benefits and the dangers associated with children accessing, and using, these types of websites and interactive services.
- Monitoring your child's online behavior is no different than monitoring your child's behavior in public and at home.

NETIQUETTE

What is it?

Netiquette ('Net Etiquette') is the use of good manners on the Internet and offers a minimum set of behaviors which organizations and individuals may take and adapt for their own use. Individuals should be aware that whoever supplies their Internet access (an Internet Service Provider through a private account, University student account, or an account through a corporation) will have regulations about ownership of mail and files, about what is proper to post or send, and how you, the user, should present yourself.

How is it used?

All users, whether a long-time user or someone relatively unfamiliar with the culture, transport and protocols of the Internet, can use these points as a guide of behavior. In general, rules of common courtesy for interaction with people should be in force for any situation, including on the Internet.

- Do not type in all caps which can imply shouting. Use symbols *, ☺ for emphasis and tone of voice.
- Do not leave the 'Subject' field blank. Mail should have a subject heading which reflects the content of the message.
- Avoid using colored text and backgrounds in your communications. Many computers have different settings that make the formatting impossible to read.
- Use Blind Carbon Copy (BCC) when sending to many recipients. This is an issue of privacy and keeps information personal.
- Watch Carbon Copies (CC) when replying. Do not continue to include people if the email has become two-way. Remember that negative comments can potentially reach unwanted eyes.
- Always include an introduction or greeting (e.g. Dear Friend,) and conclude with a closing or farewell (e.g. Sincerely, Cordially).
- Use the proper capitalization and punctuation that you would use in a letter.

- Do not forward jokes, chain letters, etc. unless your recipient has indicated that they are wanted.
- All private email is considered to be copyrighted by the original author.
- Assume that mail on the internet is not secure. Do not put anything in an email that you would not put in a postcard.
- Use of the 'Return Receipt Request' should be limited to the most important situations.
- Always minimize or *zip* large files before you send them.
- **Flaming** (heated, argument-provoking messages) is in violation of most Internet Service Provider contracts. If you receive a nasty email, do not respond immediately or at all.
- Do not forward virus warnings. This is the most popular way to spread a virus. Check a reputable website such as www.snopes.com for trustworthy virus information.
- Avoid forwarding information that you cannot verify as true. Urban myths and financial scams abound on the Internet. Use websites such as www.snopes.com to verify web lore.
- Never give out personal information until you confirm that the recipient is reputable.
- Make an effort to find the information you want on the website before you send an email. 'FAQ' and 'About Us' sections on a website are devoted to answering popular questions.
- Do not forget that the learning curve on the Internet is constantly emerging.

EMAIL

What is it?

Email is a system for sending and receiving messages electronically over a computer network between personal computers.

How is it used?

Email has proven to be a fast, convenient way to communicate in today's day and age. Email allows people to send and receive information any time of day or night, which eliminates the need for phone calls or the conventional postal system. It is also a very powerful way to communicate with a large or small group of people in a short period of time, and it can help eliminate the need for paper, which makes it environmentally friendly.

Safety Concerns

- Safety concerns with email include, but are not limited to: predators, bullying, invasion of privacy, and malicious software (*malware*).
- Email can also be a fast way to spread computer viruses, *worms*, *Trojan horses* and *bot armies* (malware).
- Emailing is used for identity theft (*phishing*), spreading scams, spam, hoaxes, and launching *spyware* invasions.
- Attachments sent in emails often contain viruses, worms or spyware so it can be difficult to determine what is safe. While you may recognize the sender's address, some emails are actually sent by infected machines that can "steal" someone's address list (*spoofing*).
- Forwarding emails without deleting or editing other recipients' addresses or personal information, leaves them vulnerable to people they do not know (*spamming*). Some spammers actually prey on these email lists to gather new addresses.
- Emails can also be retained indefinitely or shared with other people – with, or without, permission. Sensitive and/or private information or data can be passed along, printed out and distributed, again, with, or without, permission.

- Messages can be disguised and can appear as if they have been sent from a reputable company or organization, when, in reality, they have not (*transparent email*).
- Email messages are not usually encrypted and may travel through another or several other computers before reaching their destination. This makes it relatively easy for others to intercept and read messages. Many service providers store copies of email on their servers before they are delivered. Deleting messages on your computer does not delete them from the Internet Service Provider's server.
- Without computer protection (*anti-virus software, firewalls*, and anti-spyware programs), common sense and general knowledge, many people will unknowingly "infect" their own computer – as well as the computers of others with whom they communicate.
- Using public Internet-access computers in libraries, Internet cafes, etc. can leave you open to trouble since many do not have up-to-date firewalls or anti-virus packages.
- It is easy to set up an email account; many sites offer free email (like Yahoo, Google) that children or teens can access from the site's home page. Children and teens may have several active email addresses through many of these sites.
- *DSL*/Cable Internet service can also make computers, including wireless, an easy target for hackers. High-speed Internet connectivity, while popular, is very easily "tapped" into by technically savvy teens. It is advisable to unplug the cable or phone line from the computer when you are not using it to discourage the chances of hackers accessing your PC. Software designed to protect users from PC predators and/or hackers is no guarantee that computers will be safe, even when updated frequently. It will offer more protection than if no firewall software is used.
- When children are young and want to communicate via email, it is advisable to set them up with a family account until they are old enough to make educated judgments

regarding the responsible use of email. Children and teens may innocently open attachments that can be extremely harmful to computers. Not only can the PC be harmed, but the content in the emails may not be appropriate for young eyes and minds.

INSTANT MESSAGING (IM)

What is it?

Instant Messaging is a text-based form of electronic communication, which involves immediate correspondence between two or more users who are online simultaneously.

How is it used?

Instant Messaging can be used in the workplace, socially, in online gaming situations, and others. It is faster than email and enables multitasking in a way that a telephone call does not.

Instant Messaging requires a computer, cell phone, PDA or other device capable of sending and receiving text messages, and software. The software is free and can be downloaded via the websites of companies that provide such services. America OnLine (AOL), Microsoft, and Yahoo are examples of companies that offer IM software.

Safety Concerns

- There is no way to confirm a user's identity online. Any person can assume a different identity without any repercussions from any type of authorizing body.
 - Never give out personal information. Predetermine what information is considered personal.
 - Never meet anyone in person that you've met online.
 - Notify the police if an online acquaintance that you do not personally know starts to call the house or arranges a meeting.

- Ask questions about your children's online friends (Buddies).
- Investigate the many filtering and monitoring software packages available.
- Instant Messaging accounts should be set up in the parent's name using the parent's email as the contact information.

Caution

- 'Stranger Danger' (being cautious about someone we meet in person) is something we speak to our children about from the time they start to walk. Stranger Danger on the Internet should have the same priority.
- Do not accept candy from strangers. An attachment is Internet candy.
- Instant Messaging that occurs in chatrooms may or may not be monitored. A chatroom is similar to an old time "party line" on the telephone.
- We teach our children to avoid fights on the playground. Online provocation of fights is called flaming. Flaming violates terms of service with providers. Children need to be encouraged to "log off" right away if they encounter flaming.
- Just as in real life, students need to learn Netiquette. Make a point of teaching good online manners. (*See Netiquette p. 17.*)
- Many online games have chat rooms, so children and teens may be playing against, and chatting with, anyone.
- Set a time limit for online messaging.
- Tell your children to walk away and tell an adult if something does not feel right.

WHAT ARE THE WARNING SIGNS THAT YOUR CHILD MIGHT BE AT RISK ONLINE?

What is it?

Warning signs are behaviors to be aware of in your child that may be indicating that he or she is at risk or in danger online.

Safety Concerns

By keeping a computer with Internet access in a common area of your home and not in a child's bedroom, and by continually monitoring your child and referencing the following list, you can be aware of important warning signs:

- **Your child spends large amounts of time online, especially at night.** Although children and teens gain valuable knowledge and experience being online, parents should consider monitoring the amount of time spent online. Most children who fall victim to computer sex offenders spend large amounts of time online, particularly in chatrooms. They are at the greatest risk when they are online during the after-school and evening hours because offenders, who may work during the day, spend their afternoons and evenings online trying to locate and lure children.
- **Your child becomes withdrawn from the family.** Computer sex offenders will work very hard at driving a wedge between a child and his/her family or at exploiting this relationship. They will accentuate any minor problems at home that the child might have and become sympathetic listeners. Children may also become withdrawn if they have been sexually victimized.
- **Your child turns the computer monitor off or quickly changes the screen on the monitor when you come into the room.** This is a sign that your child may be looking at pornographic images, having sexually explicit conversations, or violating the parent/child agreement you both have signed.
- **You find pornography on your child's computer.** Pornography is often used in the sexual victimization of children. Sex offenders often supply their potential victims

with pornography as a means of opening sexual discussions and for seduction or *grooming*. Child pornography may be used to show the child victim that sex between children and adults is “normal.” Parents should be conscious of the fact that a child may hide the pornographic files on disks or CDs. This may be especially true if other family members use the computer.

- **Your child receives phone calls from someone you do not know or is making calls, sometimes long distance, to numbers you do not recognize.** Talking to a child victim online is a thrill for a computer sex offender, but the ultimate goal may be to talk to the children on the telephone. They often engage in “phone sex” with the children and often want to set up an actual meeting for real sex. A child may be hesitant to give out his/her home phone number, but the computer sex offenders will give out theirs and use Caller ID to find out the child's phone number. Some computer sex offenders have even set up toll-free 800 or 888 numbers so that their potential victims can call them without their parents finding out. Others will tell the child to call collect. Both of these methods result in the computer sex offender being able to find out the child's phone number. With the phone number, the predator can easily determine the child's address.
- **Your child receives mail, gifts, or packages from someone you do not know.** As part of the seduction or grooming process, it is common for offenders to send letters, photographs, or gifts to their potential victims. Some computer sex offenders have even sent plane tickets for the child to travel across the country to meet them.
- **Your child is using an online account belonging to someone else.** Even if you do not subscribe to an online or Internet service, your child may meet an offender while online at a friend's house or at the library. Most computers come preloaded with online and/or Internet software, and computer sex offenders may also provide potential victims with a computer account for communications with them.

WHAT SHOULD YOU DO IF YOU SUSPECT YOUR CHILD IS COMMUNICATING WITH A SEXUAL PREDATOR ONLINE?

What is it?

If you do suspect your child is communicating online with a sexual predator, there are steps that you can follow to try and find out.

How is it used?

By referencing the following list, talking with your child, and contacting proper authorities you can provide resolution to an online situation.

- **Do not yell, scream, or panic!** Calmly gather all the facts. Talk openly with your child about your suspicions and tell him/her about the dangers of computer-sex offenders.
- **Review what is on your child's computer.** If you do not know how, ask a friend, co-worker, relative, or other knowledgeable person. Pornography, or any kind of sexual communication, can be a warning sign.
- **Use the Caller ID service to determine who is calling your child.** Most telephone companies that offer Caller ID also offer a service that allows you to block your number from appearing on someone else's Caller ID. Telephone companies also offer an additional service feature that rejects incoming calls that you block. This rejection feature prevents computer sex offenders, or anyone else, from calling your home anonymously.
- **Consider purchasing a device that can show telephone numbers that have been dialed from your home phone.** Additionally, the last number called from your home phone can be retrieved provided that the telephone is equipped with a redial feature.
- **Monitor your child's access to all types of live electronic communications (i.e., chatrooms, instant messages, etc.), and monitor your child's email.** Computer sex offenders almost always meet potential victims via chatrooms. After meeting a child online, they

will continue to communicate electronically often via email.

- **Contact the Easton Police (261-4111) or the FBI who can help you investigate, and if substantiated, arrest an offender.**

IDENTITY THEFT

What is it?

Identity theft occurs when someone steals personal identifying information, which may include a name, address, Social Security number, date of birth, and mother's maiden name, to gain access to a person's financial accounts.

How is it used?

With this information, anyone can open new credit or financial accounts, apply for loans, rent an apartment or set up utility or phone service in someone else's name.

You can protect yourself by protecting your information. Do not give out personal information on the phone, through the mail, or on the Internet unless you have initiated the contact or are sure you know the parties with whom you are dealing. Identity thieves are clever and have posed as representatives of banks, Internet Service Providers (ISPs), and even government agencies to get people to reveal their Social Security number, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its *URL* in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Call customer service using the number listed on your account statement or in the telephone book.

Place passwords on your credit card, bank, and phone accounts and avoid using easily available information as those passwords. Examples of what not to use are: your mother's maiden name, your

child's name, your birth date, the last four digits of your Social Security number, your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Ask if you can use a password instead.

Ensure that your personal information is stored in a secure place in your home. This is especially important if you have roommates, employ outside help, or are having work done in your home.

You should routinely monitor your credit report and financial information. An amendment to the *Federal Fair Credit Reporting Act* requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit reports, at your request, once every 12 months.

Visit www.annualcreditreport.com to order your free annual report from one or from all of the national consumer reporting companies. Do not contact the three nationwide consumer reporting companies individually; they provide free annual credit reports only through this website. You can also call toll-free 877-322-8228, or go to www.ftc.gov/credit and print out the Annual Credit Report Request Form. The completed form can be mailed to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Safety Concerns

- Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.
- Before you dispose of a computer, delete all the personal information stored in it. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive.
- Some companies offer insurance or similar products that claim to give you protection against the costs associated with resolving an identity theft case. Be aware that most

creditors will only deal with you to resolve problems, so the insurance company in most cases will not be able to reduce that burden. As with any product or service, make sure you understand what you are getting before you buy. If you decide to buy an identity theft insurance product, check out the company with your local Better Business Bureau, consumer protection agency, and state Attorney General to see if they have any complaints on file.

CHAT ABBREVIATIONS

AAMOF	As a matter of fact
ADN	Any day now
AFJ	April fool's joke
AFK	Away from the keyboard
ASL?	Age, sex, location?
AYOR	At your own risk
B4N	Bye for now
BAK	Back at keyboard
BBL	Be back later
BF	Boyfriend
BYOB	Bring your own bottle
CSG	Chuckle, snicker, grin
CU	See you
CWYL	Chat with you later
CYA	Cover your ass
DIKU?	Do I know you?
DTRT	Do the right thing
ESAD	Eat sh** and die
F2F	Face to face
FOAF	Friend of a friend
GDW	Grin, duck, and weave
GF	Girlfriend
GOWI	Get on with it
HAK or H&K	Hugs and kisses
IWALU	I will always love you
IYFEG	Insert your favorite ethnic group
JAM	Just a minute
JAS	Just a second
K	Okay
KMA	Kiss my a**

KYFC	Keep your fingers crossed
L	Laugh
L8R	Later
LABATYD	Life's a b**** and then you die
LMAO	Laughing my a** off
LMHO	Laughing my head off
LOL	Laughing out loud
LTNS	Long time, no see
LTNT	Long time, no type
LY	Love you
MOTOS	Member of the opposite sex
MOTSS	Member of the same sex
NBD	No big deal
NOYB	None of your business
NP	No problem
NTW	Not to worry
OBO	Or best offer
ONNA	Oh no, not again
OO	Over and out
OTL	Out to lunch
P911	My parents are coming!
PABG	Packing a big gun
PM	Private message
POS	Parent over shoulder
RSN	Real soon now
S	Smile
SEC	Wait a second
SETE	Smiling ear to ear
TAFN	That's all for now
TIA	Thanks in advance
TOY	Thinking of you
TSR	Totally stupid rules
WAEF	When all else fails
WB	Welcome back
WTF	What the f***
WTGP	Want to go private?
YGLT	You're gonna love this
YIU	Yes, I understand
YIWGP	Yes, I will go private

GLOSSARY

Anti-virus Software that helps to protect a computer from malicious code.

Automatic Update A service available for Windows XP and Windows 2000 that downloads updates for your operating system and allows you to install them when you are ready.

Blog Short for 'web log,' Blogs range from online journals for a particular person to "easily updated personal websites." Internet users can create Blogs to discuss any subject and Blogs are readily available to the public.

Bot Army/Bot Nets Short for 'robot networks,' they are zombie computers that are controlled by a remote master computer to make money by methods ranging from spam to extortion and can use your computer in a massive attack. A bot master can see what a person is typing, including passwords and account information. Bot nets are a global problem.

Broadband Service that allows high speed Internet access usually provided by the phone or cable company.

Browser Program that allows Internet users to interact with, and navigate, parts of the Internet known as the World Wide Web. The World Wide Web is made up of a series of servers that exchange data using specified protocols and languages that can be interpreted by a browser to create the pages with which you interact.

Buddy List A list of friends' screen names that a user can instant message with the click of a mouse. Buddy Lists are a function of most instant messaging programs and buddy lists enable users to know when people they have put on their lists are available. Using a buddy list makes it easier to contact people with whom the user chats frequently.

Bug An unintended behavior or consequence in a piece of software.

Cable Modem A device used to bring broadband Internet into homes and usually provided by the cable company.

Cache A collection of temporary files kept by a browser that may contain images, sounds, Webpages, etc. By storing these files on your computer,

it may speed up your browsing experience since the information does not have to be resent over the Internet.

Certificates Provides authenticity to a website when it is attempting to download software to your browser. Users should carefully examine the certificate to determine whether they trust the site to download software.

Chat Internet application that allows users with shared interests to gather and hold real-time text conversations. A user has a screen name, types a message, and it is displayed to other users of the chat. All chat conversations are accessible by all individuals in the chatroom while the conversation is taking place. (See Chat Abbreviations p. 26)

Chat Room A public or private space on the Internet where buddies can have lengthy typewritten conversations.

Commercial Online Service (COS) Examples of COSs are America Online, Prodigy, CompuServe and Microsoft Network, which provide access to their service for a fee. COSs generally offer limited access to the Internet as part of their total service package.

Cookie Small text file sent by a website that is stored locally on a computer.

Cyberbully A person who uses the Internet for the purpose of harassing or emotionally harming other people. Cyberbullies may use Internet features such as chatrooms, Blogs, or create hate sites, etc. to hurt their victims.

Dial-up Method of accessing the Internet over a standard phone line. A slow way to connect to the Internet.

Digital Any form of information that can be stored as a series of 1's and 0's that is able to be recreated by a computer. Over the last decade, music, pictures, and video have all been stored in a digital format allowing for easier storage and sharing.

Download To copy information from another site on the Internet. Usually refers to a computer program, music, video, etc. copied from one computer to another.

DSL (Digital Subscriber Line) A form of broadband Internet provided by the local phone company.

Email Short for 'electronic mail,' it allows a user to send messages from a computer to one or more recipients over the Internet. Email is stored on a server where it will remain until the addressee receives it.

Ethernet A type of networking technology for local area networks where coaxial cables carry radio frequency signals between computers.

Favorites Section of a browser that contains a list of sites that the user has collected for future reference.

Firewall Piece of software or hardware that helps prevent hackers, viruses, and worms from reaching your computer over the Internet.

Flaming Online provocation of fights.

FTP File Transfer Protocol. Allows Internet users to upload and download large files.

Grooming The process by which an online child predator prepares a child victim by supplying him/her with pornography.

Hacker A person who uses the Internet to break into a computer or network without authorization, often causing damage.

History List in a browser that shows which sites the user has visited.

HTML Hyper Text Mark-up Language. It is the code that is sent from Web servers to browsers.

Install The process of loading a program onto a computer.

Instant Message (IM) A form of private real-time Internet text communication between two people using an instant messaging application.

Intellectual Property This is a big term and covers lots of information. It can refer to books, music, movies, videos, etc. that may be available on the Internet. It is illegal to freely distribute intellectual property without permission of the copyright holder.

Internet An immense, global network that connects computers via telephone lines and/or fiber networks to storehouses of electronic

information. With only a computer, a modem, a telephone and a service provider, people from all over the world can communicate and share information with little more than a few keystrokes.

Internet Explorer A popular browser available from Microsoft Corporation.

Internet Service Provider (ISP) A vendor that provides Internet access to its customers, and may provide broadband through cable or DSL, or offer dial-up service through a standard phone line. Examples of ISPs are Erols, Concentric, and Netcom. These services offer direct, full access to the Internet at a flat, monthly rate and often provide electronic mail service for their customers. ISPs often provide space on their servers for their customers to maintain World Wide Web (www) sites. Not all ISPs are commercial enterprises; educational, government, and nonprofit organizations also provide Internet access to their members.

Intranet System of websites that is available only to users on a specific private network. Companies often create intranets to help provide information and resources to their employees that is not available to the general public.

Leetspeak/leet A specific type of computer slang in which a user replaces regular letters with other keyboard characters to form words phonetically. Numbers and symbols often replace the letters that they resemble, letters can be substituted for other letters that might sound alike, and non-alphanumeric characters may be combined to form letters. Rules of standard English style are rarely obeyed and mistakes are often left uncorrected.

Live Electronic Communications Include, but are not limited to, chatrooms, Instant Messages, and email.

Malware Short for 'malicious software.' Refers to viruses, worms, and Trojan horses that intentionally perform malicious tasks on a computer.

Message Board An online forum where Internet users can post comments and respond to other users. Usually message boards exist to discuss specific subjects such as stocks, sports, television shows, etc.

Modem Device used by a computer to communicate with other computers on the Internet.

Netiquette Short for 'Net Etiquette.' It is the use of good manners on the Internet and offers a minimum set of behaviors which organizations and individuals may take and adapt for their own use.

Online Community A place where users of similar interests are able to gather. Could be comprised of websites, chatrooms, message boards, etc.

Online Predator Someone who uses the anonymous nature of the Internet to find victims and eventually take advantage of them in the real world.

Open Source Community of volunteers dedicated to writing and enhancing software for the purpose of freely distributing it. When software is developed by the open source community, it cannot be sold for profit.

Parental Controls Special features or software packages that enable adults to control the online activities of their children.

Peer-to-Peer Network Method of transferring data over the Internet. Peer to Peer networks are not illegal by themselves, but are often used to swap copyrighted material illegally.

Personal Identifiable Information (PII) Information that can be used to get around the anonymous nature of the Internet and discover a user's true identity.

Pharming When criminal hackers redirect Internet traffic from one website to a different, identical-looking site in order to trick you into entering your user name and password into the database on their fake site. Banking or similar financial sites are often the target of these attacks, in which criminals try to acquire your personal information in order to access your bank account, steal your identity, or commit other kinds of fraud in your name. The use of fake websites may make pharming sound similar to phishing, but pharming is more insidious since you can be redirected to a false site without any participation or knowledge on your part.

Phishing A scam operated online. A fake website that closely mirrors a legitimate website is created, official looking email is sent out in bulk to millions of Internet users, and the scam artists hope that a few people will go to the fake website and provide personal information such as bank

account numbers and passwords. This information is then used to steal from unsuspecting victims.

Pop-up Window that opens in a browser when accessing a webpage. Pop-ups are often a form of advertising used online.

Privacy Ability to restrict the kind and amount of information that is needed to be shared online.

Search Engine A software program that searches a database, gathers and reports information that contains, or is related to, specified terms available on the Internet or a portion of the Internet.

Security Bulletin Issued by Microsoft when a security update becomes available for their software.

SPAM An unsolicited message delivered by electronic mail usually for commercial purposes. Spam is the Internet equivalent of 'junk mail.'

Spammer Someone who gathers email addresses from forwarded emails when the recipients names have not been deleted or edited. A spammer can then use these addresses in any way he/she chooses.

SPIM An unsolicited message delivered over an instant message application usually for commercial purposes.

Spoofing Emails sent by virus-infected programs which 'stole' a recipient's address list through a previous email.

Spyware Term applied to software that exhibits certain behaviors, such as advertising, collecting personal information, or changing the configuration of your computer--generally without appropriately obtaining your consent.

Tag A keyword that is used to organize webpages and objects on the Internet, commonly used on photo sharing and social websites. Tags can be used to find objects with similar properties or to organize objects and can also be a reference point within an image.

Text Messaging Users can send typed messages to cell phones, PDAs, pagers, email addresses and even watches. Instant responses are available.

Transparent Email When a user believes he/she has received an email from a reputable company or organization when in reality the email has been disguised to appear that way.

Transparent Internet Use When a user believes he/she is on one website, when he/she is really on another; the true identity of a website is hidden.

Trojan horse A program that tricks a user into installing it that carries a secret agenda. The Trojan horse, once installed, will collect personal information, lock up the computer, or perform some other malicious task.

URL (Unified Resource Locator) The name of a website that is used by a browser to reach the site.

Virus A computer program that attaches itself to other programs on your computer for the purpose of replicating itself or performing other malicious acts, such as erasing files or locking up the system.

Wiki A webpage anyone can edit.

Wireless Network The method of connecting to other computers or the Internet without the use of Ethernet cables. Wireless networks are used in homes, businesses, and high school and college campuses to allow for greater computing mobility within the environment.

World Wide Web (www) The complete set of documents on a computer network of Internet sites residing on all Internet servers that use the 'http' protocol and offer text, graphics, sound, and animation.

Worm A self-propagating computer virus embedded in a file. A worm usually takes over a computer and tries to infect other computers over the Internet.

Zip Using software to minimize the size of a file.

REFERENCES

What is it?

A comprehensive list of the websites used in the production of this manual. The list was current at the time of the publication of this manual, and is intended for reference only, and inclusion on this list does not imply or suggest endorsement of any of the websites by Helen Keller Middle School, Samuel Staples Elementary School, *Easton Operation Respect* or the *Internet Safety Committee*.

Filtering and Monitoring Software

http://kids.getnetwise.org/tools/tool_result.php3

Online Safety Sites

www.theantidrug.com

www.BlogSafety.com

Child Safety Network www.csn.org

Cyber Angels www.cyberangels.org

www.Cyberbee.com

www.Cybercrime.gov

CyberTipline www.cybertipline.com

www.Equifax.com 1-800-525-6285

Experian 1-888-397-3742

Family Tech Talk www.familytechtalk.com

FBI <http://www.fbi.gov/publications/pguide/pguidee.htm>

Federal Trade Commission

Get Net Wise www.getnetwise.com

www.ikeepsafe.org

www.InternetSafety.com

iSafe America www.isafe.org

Kids Online Resources www.kidsolr.org

www.mcgruff.org

Microsoft Security At Home

<http://www.microsoft.com/athome/security/default.aspx>

www.MySpaceSafetyTips.com

National Center for Missing and Exploited Children

www.missingkids.com

Net Family News www.netfamilynews.org

Net Smartz Kids www.netsmartzkids.org

OnGuard Online

http://www.onguardonline.gov/socialnetworking_youth.html

Safe Kids www.safekids.com

Safe Teens www.safeteens.com

Stay Safe www.staysafe.org

Stop Cyberbullying www.stopcyberbullying.com

Teen Angels www.teenangels.org

Transunion 1-800-680-7289

Web Wise Kids www.webwisekids.org

Wired Kids www.wiredkids.org

Wired Safety www.wiredsafety.org

Wired Teens www.wiredteens.org

Yahooligans! Parents' Guide

<http://yahooligans.yahoo.com/parents/>

Did You Know?

Thirty-three percent of 13-17 year-olds, and 48% of 16-17 year-olds report that their parents or guardians know “very little” or “nothing” about what they do on the Internet.

<http://www.theantidrug.com>

One of every 17 minors online has been threatened or harassed online.

<http://www.cyberangels.org/statistics.html>

An alarming 75% of children share personal information about themselves willingly over the Internet in exchange for goods and services.

<http://www.cyberangels.org/statistics.html>

One out of five U.S. teens who regularly “log on” to the Internet have received a sexual solicitation or a sexual approach over the Internet, one in 33 have been aggressively pursued sexually online.

<http://www.cyberangels.org/statistics.html>

Sixty-four percent of online teens say that most teens do things online that they would not want their parents to know.

<http://www.theantidrug.com>

Seventy-seven percent of youths are contacted by an online predator by age 14, and 22% of children ages 10 to 13 are approached online.

<http://www.cyberangels.org/statistics.html>

Only 25% of children will tell a parent about an encounter with a predator who approached or solicited sex while on the Internet, and less than 10% report sexual solicitation to legal authorities.

<http://www.cyberangels.org/statistics.html>

Only 1/3 of online households in the United States proactively protect their children and teens by using filtering or blocking software.

<http://www.cyberangels.org/statistics.html>

Cover design courtesy of Frank Pagliaro.