

**KEEPING KIDS SAFE ON THE INTERNET:  
A GUIDE FOR PARENTS**



**OFFICE OF JONATHAN W. BLODGETT  
ESSEX DISTRICT ATTORNEY**

## Internet Safety Checklist

1. Move the computer to a “public” area in your home. That is a room where family members are frequently present. For example, the kitchen, the living room, the family room.
2. You should be the keeper of your children’s passwords to their online accounts. Obtain these passwords and use them to check on your child’s online activities.

Screenname \_\_\_\_\_ Password \_\_\_\_\_

Screenname \_\_\_\_\_ Password \_\_\_\_\_

Screenname \_\_\_\_\_ Password \_\_\_\_\_

Screenname \_\_\_\_\_ Password \_\_\_\_\_

3. Learn about the Internet. Specifically sit with your child and visit sites together and take a class at a local community college or ask a friend who is knowledgeable. (See glossaries for Internet terms and chat rooms in this package.)
4. Check if your child has a profile. If so, delete it. (See directions in this package.)
5. Install blocking and filtering software on your computer. (See information in this package.)
6. Use Parental Controls from your Internet Service Provider and learn how to block Instant Messages and E-mail. (See directions in this package.)
7. Learn how to check the history on your computer (See directions in this package) and check it at regular intervals. If it has been cleared, there is a chance your child is trying to cover up on-line activity. Ask them about it.
8. Develop an Internet safety plan for your family. (See examples in this package.)
9. Pay attention to your children’s behavior on and off line. If you notice a big change chances are there is something wrong that may be computer-related. Check into it.

## Blocking and Filtering Software

While there is no substitute for your personal supervision of your child's online activity, you can help yourself by installing electronic controls on your computers. Most Internet service providers (ISP) offer parental controls, time limiting and filtering options. Review your options on your ISP's home page or contact them by phone with questions on how to take advantage of these features.

In addition you can purchase software that will perform a number of functions. These functions include blocking inappropriate words, images and web sites based on predetermined criteria such as sexually explicit material, graphic violence, inappropriate language. Also, programs can block outgoing information such as your child's name, age and address. Others will monitor activity without blocking access to information. Some programs can be customized if you have more than one Internet user in your home who require different limits.

Included in this package is a chart that shows the different features of four popular software packages from [www.wiredkids.org](http://www.wiredkids.org). In addition, you can visit [www.getnetwise.com](http://www.getnetwise.com), click on Safety Guide, then Tools for Families to access a searchable database of blocking and filtering software packages that allows you to choose which features you need.

There are also kid-friendly browsers and search engines that automatically filter out inappropriate material. Remember nothing is fool proof and therefore it is important to talk to your child about what to do if they come across inappropriate material on the Internet.

***The District Attorney's office is supplying this information as a public service and does not endorse any particular product or web site.***

**WiredKids**

**Cyber 911**

▼  
**Information**

▼  
**Safe Sites**

▼  
**Adults**

▼  
**Kids & Teens**

▼  
**Emergency Help**

▶  
**Make A Report**

▶

**Child Pornography**

**Cyberstalking**

**Other Cybercrime**

**About WiredKids**

**A Note To Parents**

**Kids & Net Law**

**Filtering**

**Online Safety**

**How You Can Help**

▶

**Ask Parry**

**Contact Us**

**Volunteer**

**Make A Donation**

**Link To Us**

**For Parents**

**For Teachers**

**For Librarians**

**For Law Enforcement**

**About Safe Sites**

**Sites by Agegroup**

**Sites by Subject**

**Nominate A Site**

**Kids Information**

▶ **WiredKidz - under 13**

▶ **WiredTeens - over 13**

▶ **Teenangels**

**Special Programs**

▶

**What We Offer**

**Kids Internet Safety**

**About The Law**

**E-mail To America**

**911 Angels**

**K9 Angels**



[WiredKids](#) > [Safe Sites](#) > Filtering Software

## Filtering Software

	CyberPatrol	CyberSitter	NetNanny	SurfWatch
By	Microsystems Software Inc.	Solid Oak Software	Net Nanny	Spyglass Inc.
Works on	Macintosh, Windows 3.1, Windows 95	Windows 3.1, Windows 95, Windows NT	Windows 3.1, Windows 95	Macintosh, Windows 3.1, Windows 95
Price	\$39.95	\$39.95	\$39.95	\$39.95
<a href="#">Filter Updates</a>	1 year included	1 year	unlimited, free	1 year included
<a href="#">Update Frequency</a>	daily/weekly	daily	monthly	daily
<a href="#">Ease of Update</a>	one-button click	one-button click	several-step process	one-button click
<a href="#">Installation</a>	simple	simple	simple	simple
<a href="#">Configuring</a>	medium difficulty	simple	medium difficulty	simple
<a href="#">Start-up</a>	automatic (invisible)	automatic (invisible)	automatic (invisible)	automatic (visible)
<a href="#">Allow enable/disable</a>				
<a href="#">Password</a>	 (prompted after installation)	 (manually set after installation)	 (prompted after installation)	 (prompted during installation)
<a href="#">Tamper Proof</a>	 (2 levels of security available)			
<a href="#">Secure Files</a>				
<a href="#">Filter Library</a>	several included	several included	several included	several included
<a href="#">Custom Sites</a>				
<a href="#">Custom Patterns</a>				
<a href="#">Customizability</a>	up to 9 children	1 child only	multi-user	1 child only
<b>Filtering Techniques</b>				
<a href="#">Web site/URL</a>				

<a href="#">Hostname/IP</a>				
<a href="#">Keyword/Phrases</a>				
<a href="#">Search Engine</a>				
<a href="#">Chat Applications</a>				
<b>Filtering Areas</b>				
<a href="#">Blocks Games</a>				
<a href="#">Protects Files/Disks from Deletion/Formatting</a>				
<a href="#">Filters Outgoing Information</a>				
<a href="#">World Wide Web Categories Filtered (can be selected by parents)</a>	violence/profanity, partial nudity, full nudity, sexual acts/text, gross depictions/text, intolerance, satanic/cult, drugs/drug culture, militant/extremist, sex education, questionable/illegal & gambling, alcohol/tobacco	adult, sexually oriented, violence, gay/lesbian, illegal/radical activities, hate/intolerance, cult/occult, sports & leisure, advertising	<i>categories not named specifically but include:</i> sexually explicit, violence, hate speech, drugs/alcohol	sexually explicit, violence, hate speech, drugs/alcohol, gambling



## Checking History

Checking the history on your computer regularly is an excellent way to track where your child is going on the Internet. If you find that the history has been cleared, this may indicate that your child has visited web sites you would not approve of.

### For Internet Explorer –

- **To view the history:**  
Double click on Internet Explorer to get in. There is a history button on the top, or you can click on "View" then "Explorer Bar" then "History". Or you can just the control key and h key together.
- **To adjust the number of days kept in the history:**  
Click on "Tools" then "Internet Options" then use the up or down arrow in the history section to adjust the number of days.
- **To clear history:**  
Click on "Tools" then "Internet Options" then click on "Clear History" button in the history section.

### For Netscape

- **To view the history:**  
Get into Netscape. Click on "Communicator" then "History" (on some versions, it is Communicator>Tools>History) or you can just enter "control + h"
- **To adjust the number of days kept in the history:**  
Use the above procedure then in the history window, click "Edit" then "Preferences" and enter the how many days you want kept.
- **To clear history:**  
Do the "adjust the number of days kept" procedure then click on "Clear History" button

If you use 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.

**Source: [Familyinternet.about.com](http://Familyinternet.about.com)**

## Blocking Unwanted Instant Messages and E-mails

Instant Messaging (IM) and E-mail are probably the most widely used applications on the Internet. Examples of IM programs include: Yahoo Instant Messenger, MSN Messenger, ICQ, and AOL Instant Messenger (AIM). Examples of E-mail programs include: AOL, MSN, Juno, Hotmail, Yahoo. Remember that the screen name and password for IM and E-mail are separate and distinct. If you have AOL E-mail and IM, your child will have a *different* screen name and password for each even though they are both "America On Line."

*It is important to know that someone you do not know can contact you via E-mail or IM.* Therefore, it is important for you to get a list of your children's on-line friends screen names and know who these people are. Also you must instruct your children not to respond to a message from someone they do not know.

Another potential hazard of these applications, particularly IM, is its use to harass or argue with another person or persons. Often these "IM fights" escalate and carry over to the school environment. See a discussion about on-line fights later in this package.

There are ways to control the Instant Messenger and e-mail activity from your computer. You may block specific screen names or e-mail addresses from accessing you or your child. You may select only the screen names or e-mail addresses you want to contact you or your child.

Each IM and e-mail software program has a different set of directions to establish a blocked user list. Generally speaking, you must go into your Instant Message and E-mail program (remember they are separate so you have to do both) and select one of the following items "Mail Controls", "Parental Controls", "Privacy", "Setup" or "Preferences." If you are uncertain, contact your Instant Messenger or e-mail provider directly for guidance.

## Profiles

When you register for Instant Messaging or an e-mail account, the providers ask for a lot of personal information. Unless you are careful, that information may be publicly posted. That means you'll be sharing personal information with others without even knowing it. Information in profiles can be searched. Your child may think that kids who share their interest in a certain music performer will be able to find them easily to discuss their common interest. Remember that just as easily a predator can locate all 15-year-old girls in a certain geographic area and then use your child's interests listed in the profile to "groom" them.

Check to see that you or your child have not placed your personal information anywhere in your IM profile or used it in your registration. If you have you may edit the profile to delete this information. Go to "Privacy" or "My Status". If you cannot figure it out contact the company of the software and ask them to remove it from your profile. If they do not do so, ask them to delete your account. Reregister yourself and children again using a different address and screenname.

(Source: [www.wiredkids.org](http://www.wiredkids.org))

## Meeting Someone Online

The most serious problem imaginable is a child who turns up missing or is molested as a result of an online contact. Most of these cases are not strangers bursting into homes and stealing young kids; they are almost all young people who have left home on their own volition, usually after "meeting" someone online ("luring" is the term for online behavior that leads to these meetings). The vast majority of them are over 15 and female. What we have here isn't a case of bad guys snatching children; it's mainly teenagers exercising poor judgment. Nevertheless, luring is illegal, and if your child meets someone online whom you perceive to be a threat to her physical safety, contact law enforcement. Options (not necessarily recommendations) for preventing your child from meeting someone online who might do harm:

- Parents should take an interest in a child's "e-pals" just as they do with friends that kids bring home.
- Talk with your child about the dangers of getting together with someone they "meet" online.
- Restrict or monitor your child's use of chat functions.
- Monitor your child's e-mail and use of Internet newsgroups.
- Install a filter that restricts your child from giving out his or her name, address, and phone number.

## Getting Into Online "Fights"

People sometimes get angry. It's normal, nothing to be ashamed of. The trouble with expressing anger on the Internet is that it's sometimes difficult to resolve disputes. For one thing, you don't have the normal clues you get when you're with someone in person. When people are communicating with text, or in writing, sarcasm and some humor can be insulting instead of funny. It's difficult to know the intensity of someone's feelings and it's very hard to resolve emotional disputes that occur online. This sort of "fight" often continues once those involved go back to school, which is disruptive to the school environment and can result in disciplinary measures at school.

The best defense is to avoid getting into online arguments or disagreements. That doesn't mean people shouldn't speak their minds in forums, newsgroups, and chat sessions, but it does mean that you should treat others with respect and try not to use words that could be offensive to others. If you are going to use humor or sarcasm, you can sometimes avoid misunderstandings by using emoticons (smileys) that express emotions: A simple ":-)" (for "grin") (see "Glossary of Chat Room Acronyms") next to a statement can make all the difference between a hostile response and a collective laugh.

## Ways to prevent kids from getting into online fights include:

- Discuss with kids how to deal with anger.
- Consider counseling, if kids have serious problems dealing with anger.
- Inform kids that it's not their fault if someone is rude, obnoxious, belligerent, or mean.
- Teach your kids not to respond to comments that are mean and provocative.

(see also "Tips to Help When Your Child is Being Bullied Online" on [www.missing.kids.com](http://www.missing.kids.com), click on NetSmartz, then Parents and Educators.)

## Inappropriate Material

Just as in any city, there are areas in cyberspace that are not necessarily appropriate for children or teens. Just what those places are depends on the child, the family, and the community, but these typically include sites which are sexual in nature, which contain violent or hateful material, or which advocate the use of weapons or harmful substances such as alcohol, tobacco, or illegal drugs. Options (not necessarily recommendations) for preventing your child from being exposed to inappropriate material include:

- Set rules about where kids can go online and what to do if they stumble upon inappropriate sites.
- Keep any connected computer in a public area of the house (not a child's bedroom), and make sure that other family members walk in the room periodically.
- Consider not allowing children and teens to use the Internet if parents aren't home. You may wish to consider using time-limiting software to make sure that kids can go online only when you're around.
- Consider checking the browser history to see where kids have been and having a "talk" if they are visiting inappropriate sites. (see "Checking History")
- Consider installing monitoring software that tracks where kids have been.
- Consider installing filtering software that blocks kids from visiting sites that you feel are inappropriate.

## The Law

Kids aren't just potential victims. They can also be responsible for doing things that can hurt other people. This can range from being rude and obnoxious to committing crimes online. There are several reported cases of kids getting into trouble for posting threatening or harassing material on Web pages, in chat rooms and in newsgroups. A recent case locally resulted in a high school senior being expelled from school and being charged with making threats. Kids should remember that anything they say about anyone can be viewed by people all over

Keeping Kids Safe on the Internet: A Guide for Parents. Produced by District Attorney Jonathan W. Blodgett, January, 2004

the world and can have a damaging effect on the person being talked about. Kids should never post anything about another person that could in any way harm that person. That includes publishing names, addresses, or phone numbers of anyone they know. Kids should refrain from saying bad things about other people in public forums, even if they feel they are true, and even if they are angry with that person.

## **Making Threats**

It is wrong and illegal to threaten, intimidate, or harass other people regardless of whether those threats are delivered in person, on the phone, via the mail, or over the Internet. It can be especially harmful to deliver such threats in a public area such as a Web site, chat room, or bulletin board. If you or your child receive serious and frightening threats online contact your local police department. Parents should talk with their children about the proper way to behave online and with other people and stress that threatening other people is not only wrong but can get the child into trouble at home, at school, or with the law.

## **Legal Risks**

A lot of material posted on the Internet is copyrighted, which means that it might be illegal to reprint or post the material without permission. Kids need to understand that they do not have the right to re-post or distribute copyrighted graphics, music, videos, and text from Web sites without permission. This includes giving copies of the material to friends. There are some conditions where it is OK to use copyrighted material as part of a student paper or other project, but students should always check with their teacher first and cite the source of the information. Plagiarism - claiming that you wrote or drew something created by another person - is illegal, and committing plagiarism at school can be grounds for serious punishment.

(Source: [www.Getnetwise.org](http://www.Getnetwise.org))

## Resources

[www.childrenspartnership.org](http://www.childrenspartnership.org) “The Children's Partnership is a national nonprofit, nonpartisan organization that undertakes research, analysis, and advocacy to place the needs of America's nearly 70 million children and youth, particularly the underserved, at the forefront of emerging policy debates. The hallmark of The Children's Partnership is to forge agendas for youth in areas where none exist, to help ensure that disadvantaged children have the resources they need to succeed, and to involve more Americans in the cause for children.”

[www.cybercitizenship.org](http://www.cybercitizenship.org) “The Cybercitizen Awareness Program educates children and young adults on the dangers and consequences of cyber crime. By reaching out to parents and teachers, the program is designed to establish a broad sense of responsibility and community in an effort to develop in young people smart, ethical, and socially conscious online behavior.” Funded by the U.S. Dept. of Justice.

[www.getnetwise.org](http://www.getnetwise.org) “GetNetWise is a public service supported by a wide range of Internet industry corporations and public interest organizations. The GetNetWise coalition want Internet users to be only “one click away” from the resources they need to make informed decisions about their and their family’s use of the Internet.”

[www.livewwwires.com](http://www.livewwwires.com) The Vancouver, British Columbia-based company that developed “Missing” a computer game that teaches Middle School-age children Internet safety. This web site provides detailed information on this program and how it has been used around the world.

[www.missingkids.com](http://www.missingkids.com) “National Center for Missing and Exploited Children was established in 1984 as a private, nonprofit 501(c)(3) organization to provide services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. Among its missions and congressional mandates, NCMEC operates a CyberTipline that the public may use to report Internet-related child sexual exploitation. This site contains NetSmartz which has information and activities for parents, young children and teenagers related to Internet safety.

[www.safekids.com](http://www.safekids.com) “SafeKids.Com and SafeTeens.Com are projects of The Online Safety Project (OSP). OSP is operated by Larry Magid, a syndicated columnist, broadcaster and author of numerous articles about online safety. They work closely with the National Center for Missing and Exploited Children. This site offers guidance on filtering and blocking software as well as other safety information.

[www.wiredkids.org](http://www.wiredkids.org) “Wired Kids is the ultimate online safety project for kids & teens! At WiredKids we feature everything from safety information to online & off-

line projects involving organizations like [Disney](#). Everyone is welcome here. WiredKids is a one-stop safety resource for everyone who cares about keeping our children safe online. Some of our most active users are the kids themselves.”

*The District Attorney’s staff has compiled this list as a public service and does not endorse any of these sites in any way.*

# Family Internet

## Our Family's Rules For Internet Safety

### We All Agree:

We will never give out our last name, address, phone number, or any personal information. This includes sports team names, school information, and work information. We have all agreed upon user names (like cb handles or nicknames) to use while we are on the Internet.

**Real Name**

**User Name**

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

When asked where do we live, we are all going to answer: I live in

\_\_\_\_\_

(Upstate New York, or South East Kansas, or Northern Florida) I will never give out more information to anyone.

**We all agree to not give out our passwords to anyone outside of our family.** If someone finds out our password and uses it, we all could get into big trouble.

**We all agree to limit our online time, so that it doesn't interfere with other activities.** If mom or dad sets time limits, we agree to abide by them. The Internet is a lot of fun, but we will not allow the Internet to take time away from homework, housework, sports, face to face interaction, or spending time together as a family.

## **The Kids Agree:**

**I will never meet anyone in person that I have met online.** If anyone ever asks to meet me, I will notify mom or dad, immediately. The only way this would be considered is if my mom or dad was with me and the meeting was in a public place.

**I will tell my mom or dad right away if I see something that makes me feel uncomfortable.** Sometimes kids wander into sites that are not appropriate. This doesn't mean that I did something wrong.

**I will not remain on or click on that page that says, "For Over 18 Years Only."** If the page says for over 18 years only, it is because it is not for kids and I will not go any further and I will tell my mom or dad that I got to a page like that.

**I will only download pictures and files if I have my parent's permission.** Some of these files may contain dangerous viruses that will mess up the computer, so I will not do it, unless my parents know about it first.

**I will not send pictures of myself or my family to anyone online.** The only way that I am allowed to do this is if my parents say it is all right to do to send to this person and this person only.

**I will not believe everything that I see online.** I know that anyone can post information on the Internet, just because it is there, doesn't mean that it is correct. If I am in doubt of information, I will research it further.

**I agree that nothing is private on the Internet.** My mom or dad may read my mail or check the sites that I have been visiting. It isn't because they don't trust me, they just want to make sure that I am safe.

## **The Adults Agree:**

**If my child comes and tells that they saw something online that was not appropriate, I will discuss this openly with them.**

**I stay close to the computer while my child is online and I will be available to answer questions. I know that my child will have questions about how to use the Internet. If I don't know the answer, we will learn together.**

**Signed:**

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

This agreement was signed on \_\_\_\_\_

About.com Family Internet

<http://familyinternet.about.com/library/weekly/aa101499.htm>

Copyright © [2004](#) About, Inc. About and About.com are registered trademarks of About, Inc. The About logo is a trademark of About, Inc. All rights reserved.