

Some Basic Rules for You to Remember as a Parent . . .

- Make sure your child doesn't spend all of their time on the computer. People, not computers, should be their best friends and companions.
- Keep the computer in a family room, kitchen or living room, not in your child's bedroom. Remember that this tip isn't very helpful when your children have handheld and mobile Internet and text-messaging devices.
- Learn enough about computers so you can enjoy them together with your kids. Encourage discussions between you and your child about what they enjoy online.
- Teach them never to meet an online friend offline unless you are with them.
- Watch your children when they're online and see where they go.
- Make sure that your children feel comfortable coming to you with questions and don't over react if things go wrong.
- Keep kids out of chat rooms or IRC unless they are monitored.
- Discuss these rules, get your children to agree to adhere to them, and post them near the computer as a reminder.
- Find out what e-mail and instant messaging accounts they have and (while agreeing not to spy on them) ask them for their passwords for those accounts.
- "Google" your children (and yourself) often and set alerts for your child's contact information. The alerts will e-mail you when any of the searched terms are spotted online. It's an early warning system for cyberbullying posts, and can help you spot ways in which your child's personal information may be exposed to strangers online.
- Teach them what information they can share with others online and what they can't (like telephone numbers, address, their full name, cell numbers and school).
- Check your children's profiles, blogs and any social-networking posts. Social-networking websites include myspace.com, facebook.com and xanga.com. Social networks, generally, shouldn't be used by preteens and should be only carefully used by teens.
- Get to know their "online friends" just as you get to know all of their other friends.
- Warn them that people may not be what they seem to be and that people they chat with are not their friends, they are just people they chat with.
- If they insist on meeting their online friend in real life, consider going with them. When they think they have found their soul mate, it is unlikely that your telling them "no" will make a difference. Offering to go with them keeps them safe.
- Look into the new safer cell phones and cell phone features that give you greater control over what your children can access from their phone and how can contact them.

Recommended Websites for Children and Teens:

Search Engines:

Yahooligans!
askforkids.com

Cyber Information and Internet Safety:

WiredKids.org
StopCyberbullying.org
InternetSuperHeroes.org
Disney's Surfswellisland.com

Educational/Homework Help:

Awesomelibrary.org
Bookdivas.org
Cybersleuth-kids.com
Discovery.com
Nationalgeographic.org
PBSkids.org

For Health Education:

BAM.org
Kidshealth.org
Beinggirl.com

For Fun and Games:

Bonus.com PG
Disney.com PG
Clubpeguin.com PG
Funbrain.com PG
Brainbashers.com PG
Nick.com PG
Neopets.com PG
KOL.com PG
Teagames.com PG13
Miniclip.com PG13
Pogo.com PG
Gigglepoetry.com PG
Cartoonnetwork.com PG

For Boys:

Boyslife.org PG
Espn.go.com PG
Runescape.com PG13
pokemoncrater.com

For Girls:

Everythinggirl.com PG
Alloy.com PG13
Young-expressions.com PG13
Gurl.com PG13

- Ask your school librarian or the librarian at your public library for sites they recommend. Librarians and library media specialists are the guides to valuable and safe online resources for children.

Internet Safety Cyber bullying and Internet Predators Helpful Tips for Parents

- **Don't talk to or accept anything from strangers.** That's the first one we learn while growing up, and the first one we teach our children. The problem in cyberspace though is teaching "stranger danger." Online, it's hard to spot the strangers. The people they chat with enter your home using your computer. Our kids feel safe with us seated nearby. Their "stranger" alerts aren't functioning in this setting. Unless they know them in real life, the person is a stranger no matter how long they have chatted online. You need to remind them that these people are strangers, and that all of the standard stranger rules apply. You also must teach them that anyone can masquerade as anyone else online. The "12-year-old" girl they have been talking to may prove to be forty-five year old man. It's easy for our children to spot an adult in a schoolyard, but not as easy to do the same in cyberspace.

- **Come straight home after school.** Parents over the generations have always known that children can get into trouble when they wander around after school. Wandering aimlessly online isn't any different. Parents need to know their children are safe, and doing something productive, like homework. Allowing your children to spend unlimited time online, surfing aimlessly, is asking for trouble.

Make sure there's a reason they're online. If they are just surfing randomly, set a time limit. You want them to come home after they're done, to human interaction and family activities (and homework).

- **Don't provoke fights.** Trying to provoke someone in cyberspace is called "flaming." It often violates the "terms of service" of your online service provider and will certainly get a reaction from other people online. Flaming matches can be heated, long and extended battles, moving from a chat room or discussion group to e-mail quickly. If your child feels that someone is flaming them, they should tell you and the sysop (system operator, pronounced sis-op) or moderator in charge right away and get offline or surf another area. They shouldn't try to defend themselves or get involved in retaliation. It's a battle they can never win.

- **Don't take candy from strangers.** While we don't take candy from people online, we do often accept attachments. And just like the offline candy that might be laced with drugs or poisons, a seemingly innocent attachment can destroy your computer files, pose as you and destroy your friends or spy on you without you even knowing it. Use a good anti-virus, update it often and try one of the new spyware blockers.

- **Don't tell people personal things about yourself.** You never really know who you're talking to online. And even if you think you know who you are talking to, there could be strangers lurking and reading your posts without letting you know that they are there. Don't let your children put personal information on profiles. It's like writing your personal diary on a billboard.

With children especially, sharing personal information puts them at risk. Make sure your children understand what you consider personal information, and agree to keep it confidential online and everywhere else. Also teach them not to give away information at Web sites, in order to register or enter a contest, unless they ask your permission first. And, before you give your permission, make sure you have read the web site's privacy policy, and that they have agreed to treat your personal information, and your child's, responsibly.

- **We need to get to know your friends.** Get to know their online friends, just as you would get to know their friends in everyday life. Talk to your children about where they go online, and who they talk to.

- **R-E-S-P-E-C-T.** We all know the golden rule. We have a special one for cyberspace. Don't do anything online you wouldn't do offline. If you teach your child to respect others online and to follow the rules of netiquette they are less likely to be cyberbullied, become involved in online harassment or be hacked online. Remember that it is just as likely that your child is a cyberbully sometimes by accident) as a victim of one. Let them know they can trust you not to make matters worse. You have to be the one they come to when bad things happen. Be worthy of that trust.

- Remember that the new handheld and interactive gaming devices you buy have real risks to. Your children can send and receive text-messages from anyone on their cell phones or text-messaging devices and interactive games allow them to chat, on Internet phone, to anyone who wants to talk with them. The new Bluetooth devices let your child receive messages from anyone in a 300 foot range, and could be a problem if they play the new Bluetooth handheld games in a mall. Think about the features you are buying when you buy new devices for your children.

- Don't just set up the computer in the corner of their bedroom, and leave them to surf alone. Take a look at their computer monitor every once in awhile, it keeps them honest. Sit at their side while they compute when you can.

It will help you set rules that make sense for your child. It also gives you an unexpected benefit...you'll get a personal computing lesson from the most affordable computer expert you know!

It's worth the effort. When our children surf the Internet, they are learning skills that they will need for their future. They become explorers in cyberspace, where they explore ideas and discover new information.

Internet Tools Available

There are many tools available to help parents control and monitor where their children surf online. Some even help regulate how much time a child spends playing computer games, or prevent their accessing the Internet during certain preset times. I've listed the type of protections that are available. But, most of the popular brands now offer all of these features, so you don't have to choose. Recently, given parents' concerns about strangers communicating with their children online, monitoring software has gained in popularity. Although it might have its place in protecting a troubled child, it feels more like "spyware" than child protection. But it's ultimately your choice as a parent. The newest trend is to use products supplied by your ISP called parental controls. AOL's parental controls were the first of these to be developed and used. MSN 8.0 launched the first set of parental controls for MSN.

Blocking Software

Blocking software is software that uses a "bad site" list. It blocks access to sites on that list. They may also have a "good site" list, which prevents your child from accessing any site not on that list. Some of the software companies allow you to customize the lists, by adding or removing sites from the lists. I recommend you only consider software that allows you to customize the list, and lets you know which sites are on the lists.

Filtering

Filtering software uses certain keywords to block sites or sections of sites on-the-fly. Since there is no way any product can keep up with all the sites online, this can help block all the sites which haven't yet been reviewed. The software blocks sites containing these keywords, alone or in context with other keywords. Some companies allow you to select certain types of sites to block, such as those relating to sex, drugs or hate. This feature engages special lists of keywords that match that category. As with the "bad site" lists, the lists of keywords used by the filtering software should be customizable by the parent, and every parent should be able to see which terms are filtered.

Outgoing Filtering

This means that your child won't be able to share certain personal information with others online. Information such as your child's name, address or telephone number can be programmed into the software, and every time they try to send it to someone online, it merely shows up as "XXXs." Even with kids who know and follow your rules, this is a terrific feature, since sometimes, even the most well-intentioned kids forget the rules.

Monitoring and Tracking

Some software allows parents to track where their children go online, how much time they spend online, how much time they spend on the computer (such as when they are playing games) and even allows parents to control what times of day their children can use the computer. This is particularly helpful when both parents are working outside of the home, or with working single-parents, who want to make sure their children aren't spending all of their time on the computer. Many parents who don't like the thought of filtering or blocking, especially with older children and teens, find monitoring and tracking satisfy their safety concerns. They can know, for sure, whether their children are following their rules.

I recommend using monitoring software and then forgetting it's installed. Think of it as the security video camera in the corner of the bank. No one views the tapes until the bank is robbed. If something bad happens, you can play back the monitoring log and see exactly what occurred. I particularly like Spectorsoft.com, because their products can monitor all instant messaging platforms, which is the key to keeping your children safe online.

Parents have to remember, though, that these tools are not cyber-babysitters. They are just another safety tool, like a seat belt or safety helmets. They are not a substitute for good parenting. You have to teach your children to be aware and careful in cyberspace. Even if you use every technology protection available, unless your children know what to expect and how to react when they run into something undesirable online, they are at risk. Arming them well means teaching them well.