Parenting Online

What do we do when our eight-year-old knows more than we do about cyberspace? How do we guide our children safely through this new world? How do we set the rules when we don't even understand the risks? The childproof locks, seatbelts and helmets we use to help keep them safe in everyday life won't protect them in cyberspace. There we need new and different gadgets and safety tips.

Welcome to the new world of parenting online! It's your newest challenge. But don't worry...it's not as hard as you think and it's well worth the effort.

Parenthood is never easy and the ground rules are always changing. We go from playing the role of confidante, to co-conspirator, to police chief, to teacher, to playmate and back...all in the same day. We barely have the chance to catch our breath!

The things we do to make sure our children stay safe are constantly changing too. When they crawl, we learn how to keep things off the floor. Then, they pull themselves upright, we have to keep them safe from the new dangers at eye level. Training wheels have to be removed, and we have to watch while they pedal away (generally into the nearest tree). We watch their sugar intake, make sure they take their vitamins and keep small items out of their mouths.

That's our job, as parents. So the tried and true warnings, passed down from generation to generation, are repeated... "don't talk to strangers...," "come straight home from school...," "don't provoke fights...," "don't tell anyone personal information about yourself..." and "we need to meet your friends..." This is familiar territory after all. We know the dangers our kids face in the street or at the mall or in the school yard, because we faced them.

As in any large community, there are dangers our children encounter in cyberspace, too. But, since our children know more than we do about cyberspace, we worry about how we can teach them to avoid those dangers. Don't panic... those dangers can be managed using the same old warnings we've always used.

We just need to translate them into cyberspace terms...

And there are wonders around every cyber-corner too...

The Internet is the largest collection of information in the world, always available without a charge and delivered to your home computer. Every question you might have can be answered online. When your child asks you how deep the ocean is or why the sky is blue, you can "ask the Internet," together.

You and your children can communicate with others too, worldwide and in every language, with the click of your mouse. Their artwork can be displayed, their news reporting published and their poems posted on the largest "refrigerator door" in the universe, where 700 million people can appreciate them.

You can research your family tree and build a family Web site. And, best of all...the most complicated homework assignment can be researched online (even last-minute on the Sunday night before it's due).

You can search online for just about anything and any information you want. The easiest way to do that is by using search engines. You can type your search into one of the search engines and often will find what you are seeking. Just as often, though, you will find sites that are trying to get your or your children's attention. Pornographers are the most frequent abusers of search engines, registering and coding their sites to trick people into visiting them, thinking they are Disney, Pokemon or even the White House.

Most of the search engines now have filtering options. By selecting one of these options, most inappropriate content is filtered out and the search results are typically kid-friendly. Two commercial search engines were designed just for kids, though, and are wonderful places to begin your child's search online. Yahooligans!, Yahoo! kid-sized search engine hand-selects the sites, making sure nothing slips through. It is best for younger children, ten and under. Ask Jeeves for Kids is Ask Jeeves kid-sized search engine. Although not as scrubbed clean as Yahooligans! hand-selected sites, it contains many more sites which make it perfect for slightly older children. I recommend it for children ten and older.

In addition, most full-size search engines have a filtered option you can select. But remember that even if you use a search engine filter, if the kids search for images, the can find things you wish they hadn't. That's when using a filtering product that can block images too might come in handy.

In addition to kid-sized search engines, there are many wonderful family-friendly site lists. WiredKids has one of its own, where the sites are selected and reviewed by our specially-trained volunteers. You can even recommend your favorite sites to be added.

There are some entertaining sites that teach children online safety, as well. Although we prefer our WiredKids.org, StopCyberbullying.org and InternetSuperHeroes.org the best, (she says modestly...) another very special one we want to point out. Disney's Surfswellisland.com teaches online safety Disney-style. Mickey Mouse, Donald Duck, Minnie Mouse and Goofy all find themselves involved in tropical island cyber-challenges relating to viruses, privacy, netiquette (cyber-etiquette) and responsible surfing. Lesson plans, online safety worksheets and other wonderful resources are all available without charge at the site.

Looking for homework help? Check out Discovery.com, Nationalgeographic.org, PBSkids.org and The National Gallery of Art kids page www.nga.gov/kids/kids.htm**.** And 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. And if you need something you can't find, send me an email at "Ask Parry," (askparry@wiredsafety.org) my Internet-syndicated online safety column. Drop by WiredKids.org or WiredSafety.org to find out how to submit a question.

- **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. Period. 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 form 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. You can get a list of the ones we recommend at WiredSafety.org. Practice safe computing!

- **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. You can learn more about the ways to combat cyberbullying at our new website, StopCyberbullying.org or at WiredSafety.org's cyberstalking and harassment section. 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 form 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. Check into privacy and security settings. Our Teenangels (teenangels.org) are working on new guides for parents and other teens on what to look for and think about before you buy a new interactive device. Look for them at your local retailer or on the WiredSafety.org and Teenangels.org websites.

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!

And 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.

Also, because there is no race, gender or disability online, the Internet is the one place where our children can be judged by the quality of their ideas, rather than their physical attributes.

What Tech Tools Are Out There?
Blocking, filtering and monitoring...when you need a little help

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. To read more about the various products and services we have reviewed, visit WiredKids.org and WiredSafety.org.

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
No...this doesn't mean your software had a sparkling personality :-) (that's cyberspace talk for "grin" and means you're supposed to smile at my brilliant humor, and if you want to learn more about this stuff...you need to read my Ms. Parry's Guide to Correct Online Behavior). It 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.

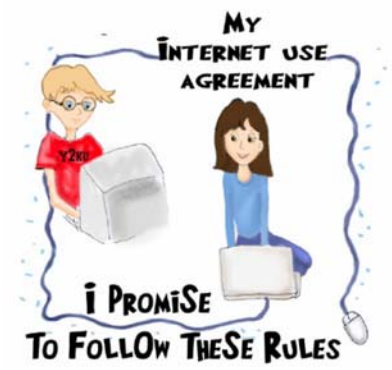
We particularly recommend using a monitoring software and then forgetting it's installed. Think of it as the security video camera in the corner of the bank. No one views the tapes until the bank is robbed. If something bad happens, you can play back the monitoring log and see exactly what occurred, and who said what, and in dire situations, where your child went to meet an adult offline. We particularly like Spectorsoft.com, because their products can monitor all instant messaging platforms, which is 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 child safety caps. 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.

Your Online Safety "Cheatsheet"
Some Basic Rules for You to Remember as a Parent . . .

- Make sure your child doesn't spend all of her 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. You can't make them keep their cell phones in a central location. So make sure that the "filter between their ears" is working at all times.
- Learn enough about computers so you can enjoy them together with your kids.
- 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.
- Encourage discussions between you and your child about what they enjoy online.
- 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. To learn how to "Google" them, visit InternetSuperHeroes.org.
- 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. (We work closely with MySpace and Facebook to help keep their users safer.) Social networks, generally, shouldn't be used by preteens and should be only carefully used by teens. Yfly.com is a new teen-only social network that is designed from top to bottom to keep teens safer and teach them about more responsible behaviors.
- For those of you with preteens and young teens, read the Safer Social Networking guide at WiredSafety.org.
- 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.

PARENTING ONLINE
MY AGREEMENT ABOUT USING THE INTERNET



Once you understand enough about cyberspace and how your children surf the Internet, you can set your own rules. These are the basic rules, even though you may want to add some of your own.

Some kids like setting the rules out clearly in an agreement. Here's one you can use, and post near your computer to help them remember how to surf safely. (Note that while the tips may work for teens, the contract is designed for preteens and younger.)

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

1. I will not give my name, address, telephone number, school, or my parents' names, address, or telephone number, to anyone I meet online.

2. I understand that some people online pretend to be someone else. Sometimes they pretend to be kids, when they're really grown ups. I will tell my parents about people I meet online. I will also tell my parents before I answer any e-mails I get from or send e-mails to new people I meet online.

3. I will not buy or order anything online without asking my parents or give out any credit card information.

4. I will not fill out any form online that asks me for any information about myself or my family without asking my parents first.

5. I will not get into arguments or fights online. If someone tries to start an argument or fight with me, I won't answer him or her and will tell my parents.

6. If I see something I do not like or that I know my parents don't want me to see, I will click on the "back" button or log off.

7. If I see people doing things or saying things to other kids online I know they're not supposed to do or say, I'll tell my parents.

8. I won't keep online secrets from my parents.

9. If someone sends me any pictures or any e-mails using bad language, I will tell my parents.

10. If someone asks me to do something I am not supposed to do, I will tell my parents.

11. I will not call anyone I met online, in person, unless my parents say it's okay.

12. I will never meet in person anyone I met online, unless my parents say it's okay.

13. I will never send anything to anyone I met online, unless my parents say it's okay.

14. If anyone I met online sends me anything, I will tell my parents.

15. I will not use something I found online and pretend it's mine.

16. I won't say bad things about people online, and I will practice good netiquette.

17. I won't use bad language online.

18. I know that my parents want to make sure I'm safe online, and I will listen to them when they ask me not to do something.

19. I will help teach my parents more about computers and the Internet.

20. I will practice safe computing, and check for viruses whenever I borrow a disk from someone or download something from the Internet.

21. I won't post my cell number on my away message, and will check with someone before posting something personal about me on my blog or on a networking site.

22. I will Stop, Block and Tell! If I am harassed online or cyberbullied.

23. I will Take 5! before reacting to something that upsets me or makes me angry online.

24. I will practice responsible "thinkB4Uclick" rules. (I know I can find out more about these things at InterentSuperHeroes.org and StopCyberbullying.org.)

25. I will learn how to be a good cybercitizen and control the technology, instead of being controlled by it.

_____

I promise to follow these rules. (signed by the child)

_____

I promise to help my child follow these rules and not to over react if my child tells me about bad things in cyberspace (signed by parent).

From Parry:

I am asked questions about kids online safety at least a hundred times a day. Is the Internet a dangerous place? Are there predators out there looking to set up a meeting with my child? How can we find good and reliable content online? How can I supervise my child's surfing when I can't even turn on the computer?

These any other question like these fill my inbox daily. (If you have a question of your own, visit WiredKids.org or WiredSafety.org and click on "Ask Parry." Here is the one simple answer:

The single greatest risk our children face in connection with the Internet is being denied access. We have solutions for every other risk.

That bears repeating, over and over, especially when we hear about Internet sexual predators, hate, sex and violence online. But our children need the Internet for their education, careers and their future.

Happily, most of the risks are easily confined. In each and every case when children encounter Internet sexual predators offline, they go willing to the meeting. They may think the person is a cute fourteen year old girl or boy, but they know they are meeting someone they don't know in real life. That means we can prevent 100% of these crimes. Merely teach our children not to meet Internet strangers offline. If they are set on meeting that person anyway, go with them. That way, if the person turns out to be a cute fourteen year old, you are the hero. And if they aren't, you're an even *bigger* hero.

Our WiredKids, WiredTeens and Teenangels programs, in addition to being fun and educational sites, are also volunteer programs where children and teens are taught online safety and privacy and responsible surfing. They then use these skills to help other children and teens learn to surf safely, as well. Talk to your children about what they do online (and offline also), and let them know you are there to help if things go wrong. You will note that in our safe surfing agreement parents have to promise only one thing...not to overreact if their children come to them for help. Earn their trust, and be worthy of it. Register your children at WiredKids.org, our children's online safety site, and we will make sure they learn what they need to know about enjoying the Internet safely and privately. It's not about technology at all...it's about communication and good parenting.

Remember, we're all in this together!

Parry
Parry Aftab, Esq.
Executive Director
WiredSafety.org and its family of sites and programs, including Teenangels.org, WiredKids.org and CyberLawEnforcement.org

WiredSafety is a 501c-3 non-profit organization formed under the laws of the State of New York. (Its legal name is "Wired Kids, Inc.")