

Keeping children safe online means teaching them to be smart, responsible users of the Internet. See tips from [WiredSafety.org's](http://WiredSafety.org) Parry Aftab.

For all age groups:

Teach your children to:

- Think before they click: With whom are they chatting or e-mailing, what are they saying and how are they saying it? Will the person on the other end know they are joking?
- Walk away from the computer and “Take 5” before responding to something that upsets them online
- Avoid spreading rumors, assisting in cyberbullying or sharing private communications online.
- Follow the golden rule of cyberspace: Don’t do anything online that you wouldn’t do in real life!

Follow responsible safety practices yourself:

- Install spyware and adware blocking software on your computer
- Make sure you have a working firewall
- Install anti-virus software and update it regularly
- Take advantage of spam-blocking tools offered by your Internet provider or e-mail software

Under 8 years old:

- Use filtering or parental control technologies. Block everything that isn’t pre-approved, rather than just filtering out the “bad” sites.
- Think about whether your children really need e-mail or IM, and if you determine they do: block all communications from anyone other than pre-approved senders and make sure their buddy list is no longer than the age of the child and that you know (in real life) everyone on it.
- Bookmark their favorite Web sites so they won’t mistype them and end up at a “bad” site.
- Use kid-sized search engines such as Yahoo!igans and Ask Jeeves for Kids.
- Limit their online time to no more than a 1/2 hour a day, unless they have a special project for school.
- Check with their teachers often for suggested Web sites and for recommendations for good resources online.
- Don’t let them use interactive games, such as X-Box Live or Sony Playstation network yet. Try Toontown.com instead.
- Sit down with them as often as possible and find out where they go online, what they like and ask or answer any questions.

- Tell them to get your permission before posting any content, including profiles and blogs, to a Web site or sending it via e-mail or IM.
- Look for safe site lists you can trust. Check out WiredKids.org’s approved safe sites list.

Age 8 to 10:

- Raise the bar on filtering or parental control technologies if you find they are complaining or are locked out of school-recommended sites. Or make sure that you use a product that will then send you an e-mail at work to let you unblock a particular site. (MSN has this feature.)
- If you add IM, make sure only pre-approved senders can send your child an IM.
- Use a pop-up blocker or toolbar (like Google’s), an antivirus program and a spyware remover (this begins the age of dangerous downloads).
- Keep using the Yahoo!igans and Ask Jeeves for Kids search engines.
- Make sure that they understand what information can and can’t be shared online with anyone.
- Practice chatting online with them so they know how to handle strangers they encounter online.
- Consider using a monitoring software to be able to review what they are saying and doing.
- Keep a close eye out for spyware in case they accidentally corrupt the files on the computer. Back everything up!
- Limit online time (aside from special school projects) to under an hour a day (including all IM and text-messaging time).

Age 10 to 12:

- Raise the bar on parental controls and filtering programs.
- Start using full-sized search engines with filters applied (check their advanced settings) or use a toolbar (Google’s comes preset with a medium filter).
- Teach them not to divulge personal information and double-check their IM “away messages” to make sure they’re not posting their cell phone numbers there.
- Make sure they can’t share pictures online, or set up profiles or blogs or webcams without your okay.
- Web sites they build should be reviewed carefully, as should screen names.
- Without going into details, warn them against predators – tell them you are concerned about people showing up at the house.
- Give them privacy as long as it is with people you trust.

- Block all but pre-approved senders.
- Interactive games should still be limited to Toontown.com and other kid-approved sites.
- Google their name, screen names, address, and telephone numbers at least once a week. Many kids post nasty things about others at this age.
- Make sure that you control the family account password and have their passwords too. Lock your private files with a password they don't know. Change all passwords often.
- In addition to watching for spyware, search your computer regularly for images (porn or of your kids), and any music, movie or media files you don't know about.
- Watch early media piracy, teach them not to steal online or offline.
- Get them started in online safety education, check out wiredkids.org or internetsuperheroes.org. Check out starting a tweenangel chapter at your local school. (For more information visit teenangels.org).
- If they have a cell phone, make sure you know its ability to play games and download images and software. Think about limiting their cell phone usage in a way that shuts it down when they exceed it, instead of just charging you extra.

Age 13 to 15:

- Respect their privacy more and talk with them about their online experiences.
- Filter sites that are inappropriate for young teens, instead of blocking all but approved sites. Some bad ones will get through, though. So talk about it beforehand.
- Give them more leeway on people they can accept IMs or e-mails from. But check and account for everyone, in real life, on their buddy list. No friends of friends.
- Make sure you filter or block image searches, which are often a way around many filters.
- Block peer-to-peer technologies and get your kids an account with iTunes or another legal music download site.
- Teach them to guard their passwords. Password theft is a serious problem at this age.
- Teach them not to pirate software or motion pictures.
- Have them Google themselves often: screen names, telephone and cell numbers, addresses, full names, nicknames, etc.
- Try and limit their use of chatrooms to monitored chatrooms or themed chatrooms on safe topics.

- Limit their online use (including text-messaging) to under 90 minutes a day aside from a special school project).
- Keep them out of social network or online dating sites such as xanga.com, friendster.com or match.com.
- Talk to them about not meeting strangers offline, and agree to go with them or teach them large group safe meeting tips (see wiredteens.org).
- Buy girls a copy of "A Girl's Life Online" (formerly known as "Katie.com") to read.
- Keep the computer in a central location and watch new interactive devices such as cell phones, text messaging devices and interactive gaming devices, like Xbox Live. Use parental controls if they come with them – Xbox does, for example.
- Consider setting up a teenangels.org chapter, or starting an online safety club at their school. (Visit Internetsuperheroes.org for available free materials.)

Age 16 or older:

- All bets are off. If they have earned your trust, give it to them. If not, unplug the computer and take away their cell phones and interactive gaming devices.
- If you haven't taught them what they need to know by now, we're all in trouble.
- Focus on teaching them to be responsible cybercitizens and to use the filter between their ears.
- Emphasize again the risks of sharing personal information and meeting strangers offline.
- Make sure they Google themselves often and report what they find.
- Teach them to use anti-virus software, to not believe everything they read online and to respect others. Check for adware or spyware often, use a firewall and teach them to come to you if anything goes wrong online.
- Ask them to help keep their younger brothers and sisters safe online.
- Remind them that you're still around if they need your help.

Source: Parry Aftab/WiredSafety.org

2008