

Social Networking Safety

A Guide for Parents

Social Networking Sites

Social networking sites are all the rage with teens. These sites provide a place for them to express their personal identity and maintain connections with friends. On these sites they can ...

- Create personal profiles.
- Post images and writings.
- Link and communicate with friends.



Why Teens May Not Make Good Choices Online

Didn't Think

Teen's brains are a "work in progress." They are biologically incapable of consistently making good choices ~ even if they want to. Learning to make good choices requires paying attention to the consequences of actions.

You Can't See Me ~ I Can't See You

- The perception of invisibility and the ability to establish anonymous accounts reduces concerns of detection ~ which could lead to disapproval or punishment.
- The lack of tangible feedback about consequences of online activities interferes with recognition that actions have caused harm and empathy for others.

Who Am I? Am I Hot?

Social networking sites have become an important vehicle for teens to explore their personal identity, values, and relationships with others. Unfortunately, this can sometimes lead to ...

- Posting outrageous material to attract attention.
- Posting material that explores emerging personal issues, including sexual identity.
- Preoccupation with the amount of electronic communication with friends.

Everybody Does It

Common online norms include ...

- "Life online is just a game ~ it's not real"
- "It's not me ~ it's my online persona."
- "I have the free-speech right to post anything I want, regardless of the harm it might cause to another."
- "If I can do it, it must be okay."

Doing What They Say

Sophisticated techniques are used online to influence attitudes and behavior. These techniques are used by commercial web sites, as well as dangerous individuals. Common techniques include offering "gifts," encouraging commitment to an individual, group, or product, creating "special" relationships, establishing an image of authority, and threatening a loss if one fails to act.

Looking For Love

Teens who are "at risk" in the real world are at higher risk online. They are ...

- More vulnerable to manipulation.
- More likely to engage in risk taking behavior.
- Less likely to listen to Internet safety guidance.
- Less willing or able to rely on parents.

Help Your Child Make Good Choices

Remain Involved

- Keep the computer in a public area of your house and pay attention to what your child is doing online.
- Keep younger children in safer places by limiting their access to pre-approved sites.
- As your child grows, gradually allow greater freedom online.
- Engage in respectful monitoring.
 - Public online activities are public and always open to your review.
 - Private communications should be reviewed only if there are reasons for concern.
 - Use monitoring software as a consequence to misuse or if you feel your child is at risk and your child refuses to talk with you.

Provide Accurate Information

Provide teens with accurate information about online risks and effective strategies to ...

- Avoid getting into a risky situation.
- Detect if they are at risk.
- Respond.

Focus on Values and Standards

Emphasize important values and standards to guide online choices. Review the Terms of Use for the sites and discuss these terms in the context of your family's values.

Respond Appropriately

Never overreact if your child reports an online concern! Fear of overreaction is the primary reason many teens do not report online concerns to adults. Help your child problem-solve an effective solution. Require your child to remedy any harm caused.

Encourage Peer Leadership

Encourage your child to be a peer leader online.

- Encourage good values in his or her online communities.
- Help friends and others if they are being harmed or are making unsafe choices.
- Report concerns to a responsible adult.

Making Good Choices on Social Networking Sites

Principal Concerns

The principal concerns associated with social networking sites are ...

- Unsafe or inappropriate disclosure of personal information or images.
- Unsafe connections with dangerous individuals or groups.
- Engage in or targeted by cyberbullying or sexual harassment.
- Addictive access.
- Lie about age to participate.

Check It Out

- Do you meet the age requirement?
- Do the Terms of Use prohibit harmful activities?
- Does the site allow you to control who has access to your profile?
- Does the site have a complaint process?

Protect Your Privacy and Reputation

- Use privacy protection features to limit who can view your profile.
 - But remember "private" does not mean PRIVATE!
- Even if you use privacy protection features, don't post material that could ...
 - Allow a stranger to find you in Real Life.
 - Attract a dangerous stranger.
 - Be used by a cyberbully to torment you.
 - Damage your reputation, friendships, or future opportunities.
 - Cause harm or distress to another.
- If someone posts this kind of information or material about you on their profile, demand that it be removed. If it is not promptly removed, tell an adult or file a complaint.
- Recognize that personality quizzes and contests are techniques to obtain your personal information for advertising.

Be Selective

- Be selective about who you add as friends.
 - When starting, limit contacts to friends and "friends of friends."
You should know how to find all of your online friends in Real Life.
- Carefully assess the safety and values of people you meet online by reviewing their profile and communications.
- Have a safe plan, approved by your parent, if you want to meet in person. Meet in a public place with a safe person nearby.
- Block anyone who ...
 - Communicates rudely.
 - Appears to be trying to manipulate you by sending "overly friendly" messages, using excessive compliments, offering you "gifts", or wanting to establish a "special" relationship.
 - Wants to talk about sex or asks for a sexy picture.
 - Does not fit your values.
- File a complaint if you receive harmful or potentially dangerous communications.

Be Responsible

- Do not send rude or hurtful messages or post harmful material.
- Respect the privacy and reputation of your friends.

Be a Leader

Speak up for good values in your online community.

If you see someone who is making bad choices or in danger ...

- Talk with the person about your concerns.
- Report to a responsible adult.

Keep Your Life in Balance

- Communicating with friends online can strengthen your friendships. But make sure you also spend time with your friends in Real Life.

Core Strategies

Effective Problem Solving

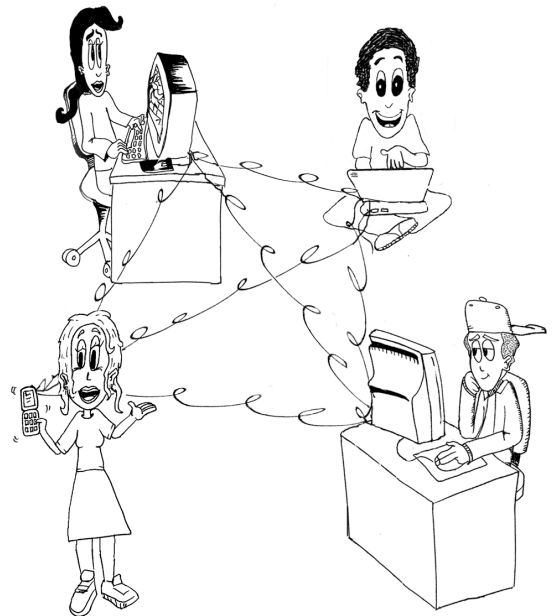
The following questions can help teens engage in problem solving.

- What is the situation?
 - What concerns does this situation raise? What are the risks?
 - What values are implicated?
- Who is involved and what are their personal interests?
 - Does anyone appear to be trying to manipulate someone else?
- What are the possible actions and the possible outcomes for each of these actions?
 - Which choice has the greatest possibility in leading to the best possible outcome for all concerned?

Responsible Decision-Making

These questions can help teens evaluate whether they are making a responsible choice.

- Is this kind and respectful to others?
- How would I feel if someone did or said the same thing to me or to my best friend?
- What would my mom, dad, or other trusted adult think or do?
- Would I violate any agreements, rules, or laws?
- How would I feel if my actions were reported on the front page of a newspaper?
- What would happen if everybody did this?
- Would it be okay if I did this in the real world?
- How would this reflect on me?



Nancy Willard, M.S., J.D., is the director of the Center for Safe and Responsible Internet Use. <http://csriu.org>. Nancy is author of *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Cruelty, Threats, and Distress* (Research Press) and *Cyber-Safe Kids, Cyber-Savvy Teens, Helping Young People Use the Internet Safely and Responsibly* (Jossey Bass).

© 2008 N. Willard. Reproduction for personal study purposes granted. A narrated presentation for parents addressing these issues, with ability to provide copies of this handout, will be available Fall 2008 on the CSRIU site.

Cybersense...translating common sense for cyberspace

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 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 spy ware 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.

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. Different types of protections are listed below that are available. But, most of the popular brands now offer all of these features, so you don't have to choose. But it's ultimately your choice as a parent. The newest trend is to use products supplied by your ISP called parental controls. Your internet provider will offer these controls free of cost.

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 prevents your child from sharing 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, and 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.

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. 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.
- 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.

KID SAFE SEARCH ENGINES AND DIRECTORIES

ASK JEEVES FOR KIDS

ASK JEEVES FOR KIDS IS A FAST, EASY AND KID-FRIENDLY WAY FOR KIDS TO FIND ANSWERS TO THEIR QUESTIONS ONLINE. DESIGNED TO BE A FUN DESTINATION SITE FOCUSED ON LEARNING AND "EDUTAINMENT," ASK JEEVES FOR KIDS USES NATURAL-LANGUAGE TECHNOLOGY THAT ALLOWS KIDS TO ASK QUESTIONS, SUCH AS "WHY IS THE SKY BLUE?" OR "WHAT'S IT LIKE TO LIVE IN SPACE?" IN THE SAME WAY THEY WOULD ASK A PARENT, FRIEND OR TEACHER. THE SERVICE COMBINES HUMAN EDITORIAL JUDGMENT WITH FILTERING TECHNOLOGY TO ENABLE KIDS TO FIND BOTH RELEVANT AND APPROPRIATE ANSWERS ON THE WEB.

AOL AT SCHOOL

AOL@SCHOOL IS A SEARCH ENGINE DESIGNED FOR EDUCATIONAL USE. IT PROVIDES LISTS OF PRESCRIBED SITES THAT HAVE BEEN SELECTED BY ONLINE EDUCATION EXPERTS. IT ALSO PROVIDES FUNCTIONAL TOOLS SUCH AS ENCYCLOPEDIAS, DICTIONARIES AND MANY OTHER RESEARCH TOOLS. THERE ARE ACTIVITIES FOR EVERY AGE GROUP. RECOMMENDED ADULT SUPERVISION FOR YOUNGER KIDS.

DIB DAB DOO AND DILLY TOO

A CHILD FRIENDLY SEARCH ENGINE THAT USES COMPUTER TECHNOLOGY TO FILTER IN APPROVED KID SAFE SITES. IT OFFERS LINKS TO ALL SORTS OF CATEGORIES FOR FUN AND LEARNING.

KIDS CLICK!

KIDSClick! WAS CREATED BY A GROUP OF LIBRARIANS AT THE RAMAPO CATSKILL LIBRARY SYSTEM, AS A LOGICAL STEP IN ADDRESSING CONCERNS ABOUT THE ROLE OF PUBLIC LIBRARIES IN GUIDING THEIR YOUNG USERS TO VALUABLE AND AGE APPROPRIATE WEB SITES.

KIDS' SEARCHING ONLINE

LYCOS ZONE IS A SAFE HAVEN ON THE WEB DESIGNED FOR KIDS, PARENTS AND TEACHERS THAT IS TARGETED TO THE NEEDS OF THE KINDERGARTEN THROUGH EIGHTH GRADE WEB AUDIENCES.

YAHOO!IGANS!

YAHOO!IGANS! IS A BROWSABLE, SEARCHABLE DIRECTORY OF INTERNET SITES FOR KIDS.