

Be reasonable and try to set reasonable expectations. Pulling the plug on your child's favorite social site is like pulling the plug on his or her social *life*. Instead of being protective, it can shut down communication and send kids "underground" where they're more at risk. It's too easy for them to set up free blogs and profiles from anywhere, including friends' houses or even a cell phone.

Talk with your kids about how they use the services. They, not news reports or even experts, are the ones to consult about their social-Web experience. Help them understand basic safety guidelines, such as protecting their privacy (including passwords), not harassing peers, never talking about sex with people they don't know, avoiding inperson meetings with people they "meet" online, and taking care in what they post - because anything people put online can be grabbed, reworked, and used against them.

Support critical thinking and civil behavior because no laws or parental-control software can protect better than a child's developing good sense about safety and relationships. Research shows that kids who are aggressive and mean online toward peers or strangers are at greater risk of becoming victims themselves. So teach them to be good citizens and friends online as much as offline.

Consider requiring Internet use in a high-traffic place in your home - not in kids' rooms - to help you stay aware of their online time. This way, you can encourage a balance between online time and their offline academic, sports, and social times. Know that there are also many ways kids can access the Internet away from home, including on many mobile phones and game players.

Try to get your kids to share their profiles and blogs with you, but be aware that they can have multiple accounts on multiple services. Use search engines and the search tools on social-networking sites to search for your kids' full names, phone numbers and other identifying information. You're not invading their privacy if they're putting personal info in public "places" online. If their pages are private, that's a good thing, but it's even better if they share it with you.



Be nice online. Or at least treat people the way you'd want to be treated. People who are nasty and aggressive online are at greater risk of being bullied or harassed themselves. If someone's mean to you, try to ignore them - often that makes them stop. Use privacy tools to block them from viewing your full profile and contacting you.

Think about what you post. Sharing provocative photos or intimate details online, even in private emails, can cause you problems later on. Even people you consider friends can use this info against you, especially if they become exfriends.

Passwords are private. Don't share your password even with friends. It's hard to imagine, but friendships change and you don't want to be impersonated by anyone. Pick a password you can remember but no one else can guess. One trick: Create a sentence like "I graduated from King School in 05" for the password "IgfKSi05."

Read between the "lines." It may be fun to check out new people for friendship or romance, but be aware that, while some people are nice, others act nice because they're trying to get something. Flattering or supportive messages may be more about manipulation than friendship or romance.

Don't talk about sex with strangers. Be cautious when communicating with people you don't know in person, especially if the conversation starts to be about sex or physical details. Don't lead them on - you don't want to be the target of a predator's grooming. If they persist, call your local police or contact CyberTipline.com.

Avoid in-person meetings. The only way someone can physically harm you is if you're both in the same location, so – to be 100% safe – don't meet them in person. If you really have to get together with someone you "met" online, don't go alone. Have the meeting in a public place, tell a parent or some other solid backup, and bring some friends along.

Be smart when using a cell phone. All the same tips apply with phones as with computers. Except phones are with you wherever you are, often away from home and your usual support systems. Be careful who you give your number to and how you use GPS and other technologies that can pinpoint your physical location.