



Rules for Online Parents

1. Personal information stays personal. Teach kids not to share passwords or give up information such as their address or school name or location.
2. Make sure your child doesn't spend all of his or her time on the computer.
3. Parents with younger kids (pre-7th grade) should try to keep the computer in a shared family space. For older kids who need to work in their own space, make sure you pop your head in often and see what they're doing.
4. Learn about computers so you can enjoy them together with your kids. Remember "because I said so" is less effective than "because I know so."
5. Make sure that your children feel comfortable coming to you in the event of an online problem. If they worry that you'll take away their computers or blame them for causing trouble, they won't come to you until it's too late.
6. Chat rooms where kids go to talk to groups of people they don't know are dangerous places—identified as places where many of the sexual predators begin their searches. Remind your children to steer clear of chat rooms. IM and social networks (when properly protected) are far safer.
7. Using the Internet is a privilege and responsibility. Consider having your children sign an acceptable use policy and let them know they'll lose computer privileges if they abuse the rules.
8. Know your children's online friends and buddies and know who they email. Know the sites they frequent. Make sure they are blocking any IMs from those not on their personal list and that you have "scrubbed" the list with them.
9. Warn them that things said on the Internet take on a life of their own and travel very quickly. They need to think seriously about consequences before pressing send.
10. Use some form of Internet filtering on your computer at least until they're old enough to begin to surf responsibly (10th grade at the earliest).
11. Warn your kids to be suspicious of people they don't know, of free deals, and of "sketchy" conversations. Tell them that if someone you never met contacts you and says, "Hi. I'm Tommy's cousin. Let's exchange photographs," a red flag should go up.

12. Remind kids that adults hiring babysitters, teachers, college counselors, and parents can use social networks, too. Don't post anything that you'd be embarrassed by in real life.
13. Arm your computer with preventative tools: a firewall, anti-virus and anti-spam software, pop-up ad managers, and junk filters.
14. Know what they do at their friends' houses, especially on the Internet. Many kids will find themselves at houses whose Internet rules are different than their own.
15. Insist your children use the privacy options available on browsers, search engines, IM, and social networking sites.

For more information visit www.robinraskin.com



A Realistic Look at Facebook and MySpace

Lots of advice about how to stay safe on social networking sites involves the words “no,” “never,” or “don’t.” Let’s try a different tack.

MySpace and Facebook are compelling places to stay in touch with your friends and rekindle old relationships, but if you’re going to use these services there are a couple of things you should be thinking about in order to protect yourself, your family, friends, and school.

- 1. Remember: Neither Facebook nor MySpace is running its site as a “not-for-profit social service.”**
 - They haven’t put up a playground solely for you to have fun, or just to be nice guys. Both sites are mega-businesses and, in part, their business relies on knowing a lot about you so they can attract the right advertisers to target you. For example, an advertiser might want to reach kids in a certain geographic area, or ones who like a certain type of music. Conversely, they can aggregate facts about you and deliver that information to their clients. It’s not necessarily a terrible thing, but it’s something you need to be aware of.
- 2. Beneath it all, Facebook and MySpace are big databases, not just a bunch of blank pages you get to decorate.**
 - Underneath everything that you fill out lives a big, huge database. That’s why it’s possible to do a search on people who meet certain requirements, say, a blond 18-year-old from Vanderbilt University. If you’ve filled in the profile questions on these sites and haven’t specified any privacy options, then your information is now part of this searchable database for *anyone* to search on.
- 3. Both sites have privacy options to protect you.**
 - Before you fill out your profile, read the options and *think about ways to keep your friends in and other people out*. You can specify what’s to be done with your photos (can other friends pass them along?) and your profile (viewable by everyone or just a select few), to name a few options. I suggest using the options that allow only those you know *for certain* are your friends to see your profile information. Others, not in your group, will only be able to see any photo or top line information you post.

4. Should you use photos?

- Pictures may inadvertently be seen (and passed along) by the wrong type of person. Many students have opted to use cartoon characters, icons, or scanned images as their photos to avoid being stalked or harassed by strangers. And don't put up any photos of your friends without telling them. They may not want the photo displayed, so be a good friend and respect their privacy.

5. What about name, address, school, and other revealing information?

- Experts have lots of different opinions about whether you're safe when you give out this information, but chances are that you're going to want to list some of these things because they are part of what defines who you are. A few suggestions:
 1. *Don't post your address.* Even with privacy options turned on, the more people with access to your address the less safe you and your family will be.
 2. *If you're using your school's name in your profile make sure that you understand your school's policy about what you can and cannot say in cyberspace.* For example, if you use the school's name and say something that might be seen as disruptive, they can—and probably will—confront you. Use your school's name in a way that they'd be proud of, not ashamed. As for your name? I'd be inclined to just use my first name or a screen name so that only my friends could identify me.
 3. *As for your age, if you're under 14 (MySpace) or 16 (Facebook), you do not belong on these sites.* That's the site's policy and it's a very reasonable one. You must fill out your age in order to be approved to be on the site.

6. How hard is it for your information to be shared against your will?

- If you use the privacy options and someone goes to look at your profile they'll *still be able to see your photo, age, and city/state of residence on MySpace.* The other parts of your profile will be hidden.

7. What if I want my profile deleted or someone is bullying me?

- Complaining to MySpace and Facebook doesn't always do much, mostly because there's always a shortage of humans to monitor and mediate requests. However, they are trying hard to honor all reasonable requests for removal of nuisances and removing profiles.

8. Can I put music and art on my profile page?

- You can't post materials that aren't yours, which often means you can't post music and artwork you may be "borrowing" for your profile page. Record companies are starting to crack down on copyright infringement of music. (If you're using music or artwork that someone else holds the copyright to, you may be depriving them of their livelihood and violating copyright law.) MySpace, for one, has publicly stated its intention to begin cracking down on these behaviors.

9. Is it safe to join a group on these sites?

- Groups can be tricky because they get polluted by people who don't belong in the group. If you are in a group with your friends on these sites you must make sure that it's *limited to people you know and trust*. Remember that it's easy for someone in a group to pass your profile information along, so don't say anything that you'd be in trouble for if it were to get out beyond the group.

10. Can my teachers, parents, etc. really see what I post on these pages?

- If you've chosen to privacy protect your profile it makes the task more difficult for non-invited subscribers to see you, though they can still see your photo, name, address, age, and school. Also, since it's relatively easy to establish fake accounts on these sites, teachers, parents, and administrators can (and sometimes do) this in order to help monitor the situation.

11. Read the terms of service.

- Look at what Facebook says about the content you put on your page, for example. It says you grant them "an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part), and distribute such User Content for any purpose on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing." That means that Facebook has a right to use what you post while you're a member of their site.

12. Don't think for a minute that things you say and show are private.

- A right click, a save page to a file, or a screenshot, and anyone with access to your page can make it exceedingly public. If you're not proud of the person your page represents then change it immediately.



A Resource Guide for Digital Kids: 2008

Compiled by Robin Raskin

Kids' Safety and Education

Wired Kids <http://WiredKids.org/>

One of the most comprehensive sites about Internet safety for parents, kids, and educators. Parry Aftab, the cyberlawyer who runs this site, has created an organization called Teenangels (<http://www.Teenangels.org/>) and trains teens to train other teens about how to avoid trouble on the Net. Teens should visit **WiredTeens.org** and get involved.

Connect Safely (<http://www.ConnectSafely.org/>) is devoted to tips, advice, and news about social networks and how to keep kids and their families safe.

i-SAFE <http://www.iSAFE.org>

Funded by the Department of Justice, i-SAFE America creates classroom curriculum and community outreach programs and programs for schools, parents, and kids. Great monthly newsletter and lots of video available from the website.

Learning About the Web

TechCorps <http://www.TechCorps.org/resources/internetsafety/getnet.htm>

Take a quiz to see how much or how little you know about keeping safe online.

NetSmartz <http://www.NetSmartz.org/>

NetSmartz was created by the National Center for Missing & Exploited Children and the Boys & Girls Clubs of America. It is one of the oldest and most comprehensive guides to Internet safety. The site has a huge library of articles about different facets of the safety question.

GetNetWise <http://www.GetNetWise.org>

A look at the various technology tools to help protect families. GetNetWise represents the collective work of a number of government and private groups working to protect kids.

NetSafe http://www.NetSafe.org.nz/offenders/offenders_default.aspx
A good discussion on grooming and how adults prey on youth on the Internet.

Family Online Safety Institute <http://www.FOSI.org/>
A sort of Internet safety think-tank, it offers a free toolbar to help parents monitor kids' access to inappropriate content and communications.

Understanding Piracy

Stay Safe Online <http://StaySafeOnline.info/>
Stay Safe Online, from the National Cyber Security Alliance, works to help protect personal and private information and has sections for parents and kids.

Business Software Alliance <http://www.BSA.org/usa/events/test-your-software-piracy-iq-quiz.cfm>
Created by the Business Software Alliance, this site contains lots of information on fighting piracy including a Test Your Software Piracy IQ Quiz.

For School Curriculums

CyberSmart! <http://www.CyberSmart.org>
An in-school curriculum created for students grades K-12 dealing with all aspects of responsible Internet use. Chapters are available as PDFs.

Consumer Awareness

The Federal Trade Commission (<http://FTC.gov/bcp/index.shtml>) can be instrumental in helping you track bad business practices involving scamming, phishing, or other malware.

Consumer Reports WebWatch <http://www.ConsumerWebWatch.org>
A Consumer Reports' foundation site that explores and reports on current Internet attitudes and problems.

Electronic Frontier Foundation <http://www.EFF.org>
The Electronic Frontier Foundation covers issues defending free speech, privacy, innovation, and consumer rights in a digital world.

Cyberbullying

Stop Cyberbullying (<http://www.StopCyberbullying.org/>) goes beyond just talking about why it occurs, to include common sense tips and the current status of the law.

Keeping Up to Date on Virus and Security Issues

SANS Institute <http://www.SANS.org/newsletters/>
The SANS Institute reviews computer security issues.

McAfee SiteAdvisor <http://www.SiteAdvisor.com/>
A free download that provides a safety rating for each site you visit on the web in real time.

Preventing Computer Crimes

ByteCrime <http://ByteCrime.org/>
Created by the National Center for Crime Prevention along with numerous partners in the non-profit, media, and high-tech sectors, the site offers information about identity theft, fraud, and other crimes on the Internet, as well as software tools and programs to make sure that you and your PC are protected.

CyberTipline www.CyberTipline.com
A site run by the National Association for Missing & Exploited Children offering basic information at its sister site, NetSmartz.org, but also offering a place to report serious acts involving missing children and predatory acts.

CyberCrime <http://www.CyberCrime.gov/>
This provides information about computer crimes and how to avoid them.

Federal Trade Commission <http://www.FTC.gov/bcp/menus/consumer/data.shtm>
The Federal Trade Commission offers a place to learn about computer fraud, identity theft, and privacy, and to report instances and problems.

Social Networking Help

ReputationDefender <http://www.ReputationDefender.com/>
A fee-based service, ReputationDefender will track your child's reputation or your personal reputation in cyberspace and work with you to clean up any problems.

