

Keeping Your Kids Internet Safe and Smart

A Survival Guide for Parents

common**sense**
media



Common Sense Media is the nation's leading non-partisan organization dedicated to improving the media lives of kids and families. We provide trustworthy ratings and reviews of media and entertainment based on child development criteria created by leading national experts. The next time you need to make a media decision, come visit us at **www.commonsensemedia.org** to help make the best age-appropriate selection for your kids.



5 Things Your Kids Do Online

A Guided Tour to the Internet

COMMUNICATING

SOCIAL NETWORKING

WEB SURFING

DOWNLOADING

GAMING

About the Ratings

Common Sense Media rates media based on developmental criteria recommendations from some of the nation's leading authorities. Our ON, OFF, and PAUSE buttons act as quick guides to help you figure out what media is right for your kids.



: Good stuff



: Think twice



: Very concerning

Keeping our kids Internet Safe and Smart is up to us

Our kids love online life, but it also gives them direct access to age-inappropriate content and risky social contacts. Since we can't always cover their eyes, we have to teach them to see. These tips will help you help your kids think critically and make good decisions about online content and communication.

5 Challenges for Parents:

1. Keeping up is hard. Online access becomes more portable every day. Sites change constantly. **Let's teach safe and appropriate behavior, not just safe and appropriate sites.**

2. Kids go online without us. They visit sites, create content, and communicate by themselves. **Let's know where our kids go.**

3. Kids know way more than we do. They've grown up online. **Kids still need ground rules and to be taught codes of conduct.**

4. It's a user-generated content world. Kids post and receive email, pictures, streaming video – all unfiltered. **Let's help our kids think critically about what they post, read, and see.**

5. We stick our noses in at a time when kids want independence. It's age-appropriate for tweens and teens to want privacy and to experiment – all of which the Internet allows. They may feel we're intruding. **Let's embrace their world, but remind them they need to be safe and smart.**

Communicating

What is it?

By middle school, online communication – email, Instant Messaging (IM), chat rooms, and blogs – leaves all other forms in the dust. Online communication is our kids' lifeline to the world – which in most cases means their friends. Kids go online to gossip, arrange social schedules, send pictures, do homework, and chat. They have email addresses and IM screen names (SNs) with passwords to protect their privacy. Kids now forward email and IMs to their cellphones (that is, when they aren't already texting on them).

Why You Should Care:

Because online communication thrives on anonymity, it can be fertile ground for cyber bullying, as well as a means for contact with people who aren't who they say they are. Since things like IM and chat rooms disappear once conversations end, no record exists of what was said, or to whom. Some chat rooms are simply bad playgrounds with predatory people lurking. And IM is one of the greatest distracters from homework in recorded history.

Hot Words:

IM

SN

Buddy list

AIM

MySpace

Xanga

Facebook

Email has become a fact of life. It affords instant communication and the ability to attach and send documents, homework, and photos.

on Email is the easiest form of communication for parents because it's searchable (if you know your kid's address and password). Some access providers have kids-only email sites – AOL has KOL, and Yahoo has Yahoooligans. Both of these sites have filters that stop spammers from jamming your kid's inbox with inappropriate ads. Email is a great way for kids to keep in touch with their friends and families and is fine for kids 8+.

II Once kids start communicating online, hazards arise. Spam, spyware, and viruses that come in email attachments forwarded by well-meaning kids can destroy a computer. Kids should never open attachments from someone they don't know.

off Make sure kids never open an email from someone they don't know or give their real names or email addresses to anyone online. People might not be who the kids think they are.

Chat rooms are online places where groups of people can carry on a conversation on certain topics. They're the hardest of the communication tools to manage.

on They can be great communities for sharing information about a common passion.

II Chat rooms tend to be theme based. Some are moderated, others aren't. No kid under 14 should venture in without you.



Because of the ease of contact and because they're often organized around titillating subjects – like sex, cults, or dangerous physical acts – chat rooms attract dangerous people who lurk there protected by anonymous screen names. A child should never reveal any personal information about their real names, addresses (email or snail mail), schools, or telephone numbers.

Instant Messaging (IM) Once kids hit middle school, Instant Messaging (or IMing) is it. Many different providers now offer this private, instantaneous form of communication. AIM (AOL's Instant Messenger) is the market leader. (Other brand names: YIM, MSN Messenger, Gtalk, and, of course, IM on MySpace.) IM lets kids create “buddy lists” of friends with whom they communicate. Since these buddies are identified only by screen names (SNs), it may not be clear to whom your kid is talking. Kids often have multiple conversations with friends going at the same time.




IM is free, and kids can be connected to their friends instantly.





IM is hard to manage. Kids change their SNs (screen names) constantly, and their buddy lists can quickly grow into the hundreds. In fact, it's a point of pride. Don't believe your kids when they tell you that they know everyone on the list. Also, unless you change the settings to archive conversations (a feature available on all major IM programs), IMs disappear the moment a dialogue window closes, making it impossible to trace. (For those who think their kids might change the settings back, there is


software that can capture IMs.) As for IM spelling? LOL! (laughing out loud)

 Kids spend hours on IM (often during homework – not a good idea). Research shows that it interferes with attention and detail. Because of the viral nature of IM, it's a great medium for cyber bullying. Kids can cut, paste, and IM cruel comments about other kids in a matter of moments. And some “buddies” can be predators. It happens.

Blog is short for “Web log.” Simply put, it's a Web page where people can post whatever they like and offer a way for others to both read and comment. Most kids create blogs on social networking sites like MySpace, Facebook, or Xanga (much more on those below). But the blogs we're talking about here are the ones that record an interest or hobby.

 Blogs can be a wonderful way for kids to be creative. Publishing a blog can be a real esteem booster and a way for kids to grow their communication abilities.

 Anyone can read a blog, download its contents, and archive it. Just because a kid takes something off a blog doesn't mean it's gone. Because blogs often serve as online diaries, kids can inadvertently give out personal information, which can make it easy for them to be contacted by strangers. Also, unsupervised blog content sometimes contains less-than-kind comments about other kids.

 Under no circumstances should any personal information appear in your child's blog. But because you may not know whether he or she has one, you might have to settle for a discussion of the fact that 1 in every 5 kids is sexually solicited online.

Common Sense Says:

1. Never reveal personal information.

No real names, birth dates, area codes, phone numbers, addresses, or anything identifiable in profiles or blogs. Screen names should be gender neutral. Explain the dangers. 1 out of every 5 kids gets sexually solicited online.

2. Never meet a stranger. Ever.

No talking, no meeting, no way. If someone you don't know makes contact, attempts to arrange a meeting, or tries to turn kids against you or their teachers, these are danger signs. This should tell you to end contact.

3. Establish codes of conduct. If your kids wouldn't say something to someone's face, they shouldn't put it in an IM or email. No flaming or cyber bullying. Emailing an embarrassing picture of someone is a form of cyber bullying!

4. Don't share passwords. Not even with friends. Ask kids for their passwords. The older ones may not want to tell you (citing privacy – that's up to you), but for middle schoolers and younger, it's AOK for you to check for inappropriate or dangerous communications.

5. Set limits on time and use. For younger kids, have the computer in a central place. Whether it's no IM during homework or no email behind closed doors, make rules. Preferably before the computer turns on.

Social Networking

What is it?

Social networks are virtual communities – basically IM (instant messaging) on steroids. They're the bulletin boards of kids' lives. Kids create their own pages with pictures and invite "friends" to join. They offer kids instant community and instant celebrity and are a handy way for trying out new identities – an activity that is both age-appropriate for teens and an essential part of growing up.

Why You Should Care:

Not everyone is a "friend." These spaces provide details about kids that sexual predators can use. It's an anonymous playground, so cyber bullying prospers as kids taunt other kids and post humiliating pictures. The language used can make a parent faint. Posts can backfire, since dubious entries can be seen by family, teachers, and employers. Finally, this is one of the greatest time eaters ever.

Hot Words:

Blog

Friend

MySpace.com

Facebook.com

YouTube.com

AIMSpace.com

Blogger.com

Xanga.com



Social networking creates online communities and gives kids a way to express themselves and test out different identities.



Parents are caught in between teens' age-appropriate need for independence and privacy and their parental need to protect. Telling kids not to post the location of a party may be met with a chilly response, but parties rapidly get out of hand when broadcast. Your kids may think that what they post is private, but anything can be viewed by anyone – including college admissions staff and potential employers, who may make acceptance or hiring decisions based on what they see. Just because a kid takes a post down doesn't mean it hasn't been captured and archived forever somewhere.



Kids' profiles, likes, dislikes, and locations become available for view by sexual predators and others who use the anonymous nature of the online world to their advantage. While some new "friends" are just who they say they are, there are no guarantees.

Common Sense Says:

- 1. Age limits.** No for middle schoolers or younger.
- 2. Balance your child's privacy and self-expression needs with safety.** Forbidding is less effective than teaching about safety and appropriate postings.
- 3. Nothing is "private."**
- 4. No personal identifiers.** No schedules, no party postings, etc.
- 5. Don't let kids meet strangers.**

Web Surfing

What is it?

Basically, your kids **connect to the Internet** through an **ISP** (Internet Service Provider) using a dial-up modem, a cable modem, DSL, or a wireless connection (WiFi). This connects them to either a service provider's **home page** (AOL) or a home page of your choosing (you can set your home page using your browser's Tools menu and selecting Internet Preferences). From there, your kids use a **browser** (Internet Explorer, Netscape, Mozilla, Safari, Firefox) to get to a **search engine** (Google, Yahoo, AOL Search) to get to a **URL** (Web address).

Why You Should Care:

The computer is their jet plane to uncharted worlds. Make sure they know how to pilot safely, because they can land just about anywhere. Kids surf to explore, push the envelope, and discover ... all sorts of things. And they can really crash your computer while they're at it.

Hot words:

Google

Yahoo

Explorer

eBay

Filters

Blocks

Pop-ups

Spyware

Crash

On, Off, and Pause



Surfing puts a world of information at kids' fingertips, which is great for research. Also, parents can track where kids have been by checking under "history" (until they get old enough to figure out how to delete the files ...).



Kids can (and will) type "sex" or "Paris Hilton" into their **Google or Google Image search** box and come up with stuff you would rather they had never seen. If you have young kids, you might want to investigate **filters** or content **blocks**. Surfing also means **pop-ups** – these are unsolicited ads that often look "official." Clicking on one opens unwelcome sites and can also install **worms, viruses, spyware, and adware** (basically, software that sneaks into your computer to track where you go on the Web and slows a computer to a crawl – or worse). Also, kids tend to believe what they read on the Internet. Not all information is correct, since anyone can post just about anything they want – accurate or not.



Surfing in an unfiltered and unsupervised environment can expose kids to really inappropriate content – violence, sex, hate, and more.

Common Sense Says:

- 1. Location.** For younger kids, have the computer centrally located.
- 2. Check history** to see what sites they've visited.
- 3. Never click on pop-ups**, enter contests, or answer questionnaires.
- 4. Investigate Internet safety software** and keep browsers up-to-date
- 5. Think smart.** Explain that Internet content isn't always accurate or true.

Downloading

What is it?

It's a simple rule: If it can be surfed, it can be downloaded. Downloading falls into two camps: the free and the not free. Free downloads include promotional music, peer-to-peer file sharing of music and videos (exchanges like **LimeWire** and **Kazaa** are illegal, iTunes is legal). Downloads that cost (and require a credit card) include games, mobile phone ringtones, music (iTunes and its competitors), audio books, TV episodes, movies, music videos, and more.


Why You Should Care:


Downloading is turning computers into relay stations for cell phones, MP3 players, and video iPods. Songs, video clips, and photographs are downloaded, then transferred to these more-portable devices. Illegal downloads can subject computers to virus attacks – and you to legal prosecution. Also, content is often not rated, and any kid of any age can have access.


Hot Words:

Limewire
Kazaa
iTunes

Streaming video
Ringtones

 Convenience and speed of access have to be the best things about downloads. Going on a car ride? Download a Harry Potter audio book and burn it onto CDs or transfer it to your kid's MP3 player. Because most legit content requires a credit card, parents are more involved than with other Internet activities.

 Most sites allow access to music, video, and games with no ratings involved. You might not know the content of what you're downloading (although iTunes and other online music stores do carry "parental advisory" labels). Also, because sites get around the credit card issue by offering "allowances," kids can download video and music that you might not want them seeing and hearing.

 Some peer-to-peer (P2P) software that allows people to share music and video files is strictly illegal. Yet kids are tempted by the offer of free music or *Simpsons* episodes. A few years ago, the government arrested kids (and their parents) for copyright infringement. While that's a long shot, it's still stealing, piracy, and a very, very bad idea.

Common Sense Says:

- 1. Set rules with your kids** about what you will and won't let them download.
- 2. Check for peer-to-peer file sharing systems.** Delete them.
- 3. Downloads cost money.**
- 4. Do your homework. Check ratings and content information.**

Gaming

What is it?

Some games are free, some are not. Some are rated, some aren't. Some require subscriptions; others, a one-time fee. Some games have side chat rooms (many with voice chat), most free games require an email address (never a good idea for kids), and all multiplayer games require screen names or character names (called gamertags), which can reveal your kid's age and gender. Games range from poker (big with high school kids) to multiplayer shooter games to innocent arcade games.

Why You Should Care:

There's absolutely no way around it: With games, adults have to be involved. Games can cost money. They're addictive and chew up vast amounts of time. Just because you don't play them doesn't mean your kids don't. Some of the content? Whoa. And kids interface with strangers in online game chatrooms all the time.

Hot Words:

Gamertags
Voice chat

Multiplayer
Chat rooms
Griefers



Games are fun and pass the time. Some are educational and sharpen reading, math, and decision-making skills.



Privacy, safety, and age-appropriate content are all a concern. Games are highly addictive time consumers. They're built so that your kids either want more or can't get far in a short period of time. This will frustrate your attempts to limit game time – but limits are a must. Many online games don't carry ratings. Many allow contact with strangers. Even if it's through a screen or gamer name, it's still contact. There's also enough bullying that cyber villains have their own name: grievers.



Sex, violence, language, and anti-social behavior are common elements in many games. Part of this world's appeal – especially for young boys – lies in the edginess of its content. A first-person shooting game or high-stakes poker match gives gamers a jolt of sensation. Games will chew up your kids' days and nights if you don't intervene. And on top of all that, games can model behavior you never want to see in your kid.

Common Sense Says:

- 1. Know game content and ratings.**
- 2. Set time and price limits.**
- 3. No personal identifiers.** This means email addresses, passwords, or gender-identifying gametag or screen names. Don't let younger kids use voice chat.
- 4. Know who your kid is playing with.** Mute or block unwanted messages, and report offenders to game administrators.

Internet Survival Tips for Kids and Teens:

1. Never give any personal information to anyone you meet online. That means first or last names, phone numbers (they can be used to track down your home), passwords, birth dates or years, or credit card information.

2. Never meet up with anyone you don't already know. Don't tell anyone your schedule; don't say where you'll be hanging out. No party announcements. People are often not who they say they are. It's true: 1 in 5 kids will be sexually solicited online.

3. Don't fill out any "fun" questionnaires that are forwarded to you, even if they're from your friends. Remember, you're in a world where everything can get forwarded. All those personal things about you could land in the hands of someone who could use them to harm you.

4. Make sure you know everyone on your buddy list. If you haven't met the people face-to-face, they may not be who they pretend to be. Also, Instant Messaging strangers is an invasion of their privacy.

5. Don't answer emails or IMs from people you don't know. Who knows who they are? Even if they say they're "David's friend," David could be a lucky guess. "Kids" you meet in chat rooms may actually be adults.

6. There's no such thing as "private" on the Internet. You may think so, but it's not true. People can find anything they want – and keep what you post – forever.

7. Be careful about posting pictures of yourself (or if you must, don't post sexy ones or ones showing behavior you wouldn't want your mom, teacher, boss, or potential college advisor to see). Just because a friend or an older sibling has posted snaps on a site doesn't make it a smart or a safe idea. Pictures with identifiers like where you go to school can be shopping lists for online predators.

8. Don't send pictures of other people. Forwarding an embarrassing picture of someone else is a form of bullying. How would you like it if someone did that to you?

9. Don't download content without your parents' permission. Many sites have spyware that will damage your computer. Other sites have really inappropriate content. Your parents can check your computer's URL history, so you can't hide where you've been.

10. Never share your password with anyone but your parents.

Remember that as frustrating as your parents are on this subject, they're only trying to keep you safe.

Internet Survival Tips for Parents and Teachers:

- 1. Be aware and involved.** It's up to us to teach kids how to use the Internet – and all media – safely and responsibly. Just as we teach them how to eat properly and drive safely, we must teach them how to be safe, responsible, and respectful on the Internet.
- 2. Do your homework.** Check out sites, investigate ratings, explore safety and privacy tools and parental control features. Don't be intimidated by the Internet.
- 3. Talk to your kids.** Ask them questions about where they're going online and who their buddies are.
- 4. Teach safety.** Make sure your kids know how to avoid dangers. No party postings, no personal information, no meeting strangers – ever.
- 5. Set rules.** Time limits, place limits, codes of conduct. Try to keep computers with Internet access in a central room in your house if younger kids are online.
- 6. Report suspicious activity** to your Internet service provider or the National Center for Missing and Exploited Children (1-800-843-5678).

7. Help kids view online information with a critical eye. Not everything that appears on the Web is true. Teach them to be savvy consumers of Internet information.

8. View your own online habits with a critical eye. Our kids watch everything we do. If you don't want your kid doing what you're doing online ... you might want to think twice about your own habits.

9. Make sure you keep channels of communication open. If your kids think they're going to lose their computers or get yelled at if they tell you something upsetting (like they've been in a sex chat room out of curiosity), then they won't come to you when they really need to.

10. Embrace their world. Download music, IM your kids, play an online game, visit MySpace and create your own profile. Not only will your kids appreciate it, you'll know what you're dealing with!

**Remember, the Internet is here to stay.
It's our job to help our kids be
Internet Safe and Smart.**



1550 Bryant Street, Suite 555
San Francisco, California 94103

©2006 Common Sense Media

Did you find this information helpful?
Let us know. Send us your thoughts to:
info@commonsensemedia.org

common  **sense**
media

www.common sense.com