Internet Safety Guidelines

- Clear, simple, easy-to-read house rules should be posted on or near the monitor. Create your own computer rules or search for an Internet safety pledge you like. The pledge can be signed by adults and children and should be periodically reviewed.
- Look into safeguarding programs or options your online service provider might offer. These may include monitoring or filtering capabilities.
- Always read a website's privacy policy before giving any personal information. Also make sure that a website offers a secure connection before giving credit card information.
- Websites for children are not permitted to request personal information without a parent's permission. Talk to children about what personal information is and why you should never give it to people online.
- If children use chat or e-mail, talk to them about never meeting in person with anyone they first "met" online.
- Talk to children about not responding to offensive or dangerous e-mail, chat, or other communications. Report any such communication to local law enforcement. Do not delete the offensive or dangerous e-mail; turn off the monitor, and contact local law enforcement.
- Keep the computer in the family room or another open area of your home.
- Get informed about computers and the Internet.
- Let children show you what they can do online, and visit their favorite sites.
- Have children use child-friendly search engines when completing homework.
- Know who children are exchanging e-mail with, and only let them use chat areas when you can supervise.
- Be aware of any other computers your child may be using. Ask questions regarding how those computers are secured or monitored.
- Internet accounts should be in the parent's name with parents having the primary screenname, controlling passwords, and using blocking and/or filtering devices. Parent's should have access to all social media accounts.
- Children should not complete a profile for a service provider and children's screennames should be nondescript so as not to identify that the user is a child.
- Talk to children about what to do if they see something that makes them feel scared, uncomfortable, or confused. Show them how to turn off the monitor and emphasize that it's not their fault if they see something upsetting. Remind children to tell a trusted adult if they see something that bothers them online.
- Consider using filtering or monitoring software for your computer. Filtering products that use whitelisting, which only allows a child access to a preapproved list of sites, are recommended. Using filters only is not enough; education is a key part of prevention.
- If you suspect online "stalking" or sexual exploitation of a child, report it to your local law-enforcement agency. The National Center for Missing & Exploited Children (NCMEC) has a system for identifying online predators and child pornographers and contributing to law-enforcement investigations.

Please see back for safety details

* Many of these suggestions are taken from www.netsmartz.org

Internet Safety Guidelines, cont.

Children whose parents and guardians regularly talk to them about personal safety are more likely to exhibit responsible behavior on their own.

Learning to recognize the warning signs of **cyberbullying, exposure to inappropriate material, online predators, revealing too much personal information** will allow trusted adults to intervene and lessen potential negative impacts. As a parent or guardian, you should stay well-informed about current issues to understand what your children are experiencing on and off the Internet. If they are social networking, instant messaging, using webcams, or blogging, help them use these tools safely by learning how to use them yourself.

Basic tips:

- Keep the computer in a high-traffic area of your home.
- Establish limits for which online sites children may visit and for how long.
- Remember that Internet technology can be mobile, so make sure to monitor cell phones, gaming devices, and laptops.
- Surf the Internet with your children and let them show you what they like to do online.
- Know who is connecting with your children online and set rules for social networking, instant messaging, e-mailing, online gaming, and using webcams.
- Continually dialogue with your children about online safety.

Start a discussion with your child.

- What are your favorite things to do online?
- What is personal information? Why should you keep it private?
- What could you do to be safer online?
- What would you do if anyone online asked to meet you face-to-face?
- Besides me, who do you feel that you can talk to if you are in a scary or uncomfortable situation?

Methods for managing your in-home technology:

- Utilize parental locks and passcodes on all Internet connected devices, including: computers, phones, iPod/iPad style devices, game consoles, DVD players, cable/satellite boxes.
- Use settings on your home router to block and/or allow websites, set content ratings, limit access times and review history logs.
- Consider setting rating limits for viewable content on cable/satellite boxes, NETFLIX, XBOX, etc....

The key to success is education. Teaching a child how to act and what choices to make when exposed to these situations will have a greater influence than any amount of monitoring and filtering.

* Many of these suggestions are taken from www.netsmartz.org

Cell Phone Safety and Monitoring

Do you think about your child's cell phone when you consider internet safety?

Smartphones have operating systems similar to that of computers which allow users to download programs or "apps." These apps help users do things like access e-mail and play games. Also, most cell phones allow users to download and upload content from the Internet just as they would on a computer. However, cell phones can be more difficult to monitor than a computer, and children often use them without adult supervision. Make sure to review your family's Internet safety rules with your children and become aware of the following risks before allowing them to own cell phones:

Making Cyberbullying More Painful

Cell phones make it easy for children to communicate with their friends, but they also make them vulnerable to cyberbullying. Cell phones can be used at anytime and anywhere, giving cyberbullies unlimited access to their victims. Children may send and receive mean-spirited phone calls, texts, and pictures at any hour.

Playing a Role in Grooming

Predators also know and take advantage of the fact that cell phones let them talk with their victims at any time. They are also aware that parents and guardians often forget to monitor children's cell phones. Predators may send children cell phones and ask them to keep the phones a secret. They can then talk to and exchange text messages and pictures with children without close monitoring by parents and guardians. Others may ask children for their cell phone numbers after meeting them online or try to connect with willing children by sending texts to random numbers.

Sexting Made Easy

"Sexting" is a term used to describe the sending of sexually explicit text messages or pictures of minors by minors. What most young people do not realize is that the production, possession, and distribution of explicit photos of minors, even if they are self-produced, may be illegal. Furthermore, if these explicit photos end up on the Internet, children may be taunted by their peers and jeopardize scholastic, athletic, and employment opportunities. Generally, once a photograph is uploaded to an Internet based platform, it will exist forever with little chance of removal.

Unintentional Sharing of Geolocation Data

Most smartphones have GPS technology which allows the user's precise location to be pinpointed by apps and on websites. Social networking sites such as FourSquare, GoWalla, and Facebook take advantage of this technology by encouraging their users to "check-in" or share their locations. A "check-in" can be shared with a list of friends, so make sure you know who is on your child's friends list before allowing them to use this type of technology. Children also may share their locations unintentionally through pictures taken with their smartphones; these photos often have geolocation data embedded in them. It is strongly recommended that you disable the location services on smartphones before allowing children to post photos online.

Please see back for safety details

* Many of these suggestions are taken from www.netsmartz.org

Cell Phone Safety and Monitoring, cont.

It is the parent's responsibility to help their child use a cell phone safely.

- Establish rules for when they are allowed to use their cell phone, what websites they can visit, and what apps they can download.
- Review cell phone records for any unknown numbers and late night phone calls and texts.
- Remind your children that anything they send from their phones can be easily forwarded and shared.
- Teach your child never to reveal cell phone numbers or passwords online.
- Talk to your child about the possible consequences of sending sexually explicit or provocative images or text messages.
- When shopping for a cell phone for your child, research the security settings that are available.
- Consider establishing a routine in which children do not take cell phones into their bedroom and leave them with the parents over night.

Start a discussion with your child.

Use these discussion starters to get an Internet safety conversation going with your children. The more often you talk to them about online safety, the easier it will get, so don't get discouraged if they don't respond immediately!

- What features do you use on your cell phone? Could you show me how to use them?
- Have you ever gotten a text from someone you do not know? If so, what did you do about it?
- Have you ever sent a text that was rude or mean?
- How many numbers do you have stored in your phone? Do you know them all in person?
- Has anyone ever taken an embarrassing picture of you without your permission?
- Have you ever taken an embarrassing picture of someone else? What did you do with it?
- Have you ever talked with someone you first met online on your cell phone?
- What would you do if someone sent you a text or picture that was inappropriate?

Check with your service provide for details on account management.

All major cell phone service providers have management tools. Most of these services are free and a few upgraded capabilities are available for a reasonable monthly cost. This can include: content filters, app blocking, time frames in which features can operate and activity monitoring.

Some parents find it necessary to use apps to monitor texting, such as SMS Spy.

* Many of these suggestions are taken from www.netsmartz.org

GOT NETSMARTZ?

CYBERBULLYING

AVOID GOSSIP.

Everyone's bound to get a little excited by those oh-so-dramatic high school scandals, but that doesn't mean you have to text the latest rumor to everyone you know.

DON'T FEED THE CYBERBULLIES.

Ignore mean or threatening messages. Block the sender and file a report with the website, cell phone service, or police.

BYSTANDERS ARE GUILTY, TOO.

If your friends are cyberbullying someone and you stay silent, you're just as guilty as they are. Speak up and keep your friends in check.

ONLINE PREDATORS

RECOGNIZE THE DIFFERENCE BETWEEN CUTE AND CREEPY.

Think about it – an older guy who wants to date someone younger is just creepy. It's not flattering; it's illegal! So don't friend them and don't meet them offline.

DON'T JUST SIT THERE – REPORT!

If you or someone you know has been victimized by someone you met online, report them to the police and www.cybertipline.com.

SHARING TOO MUCH

INITIATE OPERATION PROFILE CLEAN-UP.

Scrub your page of everything too personal, embarrassing, and illegal. Those pictures of you passed out next to the empty bottles are not going to look so cool when you start applying for college.

STOP. THINK. PUT YOUR CLOTHES BACK ON!

You know those pictures of you wearing next-to-nothing and making kissy faces or flexing in the mirror? You might think it's sexy, but the law doesn't, so do yourself a favor – don't send them; don't forward them.

PROTECT YOUR SPACE.

Use privacy settings and don't accept just anyone as a friend. Do some investigating – Who are they? Why would you hang out with them?

TRUSTED ADULTS

TALK TO YOUR PARENTS OR GUARDIANS. THEY'RE NOT AS UPTIGHT AS YOU THINK.

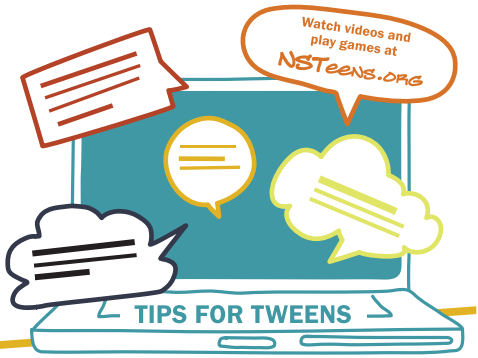
Sometimes adults freak out about what you're doing online because you never tell them anything. Keep them in the loop so they know they can trust you.

NetSmartz Workshop

A PROGRAM OF THE NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

Watch Real-Life Stories videos at NSTeens.org

YOUR NETSMARTZ



CYBERBULLYING

Don't be mean.
Gossiping doesn't make you cool.

Ignore. Block. Tell.
Ignore mean or threatening messages, block the sender, and tell a trusted adult who can help you report them.

Speak up
if your friends are cyberbullying someone.

ONLINE PREDATORS

Recognize the difference between cute and creepy.
An older guy who wants to date someone much younger is just creepy.

Don't just sit there – REPORT
anyone who asks to meet you in person to the police and www.cybertipline.com.

SHARING TOO MUCH

Avoid TMI.
Don't post anything too personal or embarrassing.

Protect your space.
Use privacy settings and don't accept just anyone as a friend.

Don't be that kid
who gets suspended for posting something stupid online.

TRUSTED ADULTS

Talk to your parents or guardians
about what you're doing online. They're not as bad as you think.

tips to prevent SEXTING FOR TEENS

NetSmartz.org/TipSheets

THINK ABOUT THE CONSEQUENCES

of taking, sending, or forwarding a sexual picture of someone else, even if it's of you. You could get kicked off of sports teams, face humiliation, lose educational opportunities, and even face a police investigation.

NEVER TAKE

images of yourself that you wouldn't want everyone—your classmates, your teachers, your family, or your employer—to see.

BEFORE HITTING SEND

remember that you can't control where this image may travel. What you send to a boyfriend or girlfriend could easily end up with their friends, and their friends' friends, and so on…

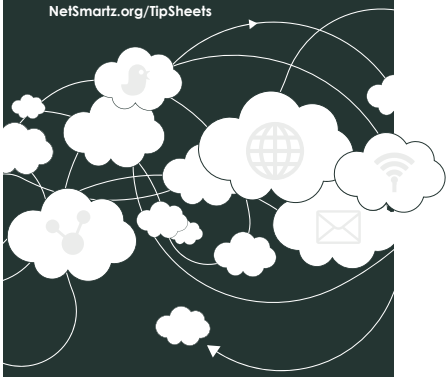
IF YOU FORWARD

a sexual picture of someone without their consent, you are violating their trust and exposing them to potential ridicule. It's not up to you to decide who should see their body, so don't forward the image to anyone.

IF ANYONE PRESSURES

you to send a sexual picture, don't give in and talk to an adult you trust. Remember that anyone who tries to get you to do something you are uncomfortable with is probably not trustworthy.

NetSmartz.org/TipSheets



Protecting your KIDS on social media

Online social media services aren't new, but many of us are still learning how to use them without getting into trouble – especially children and teens. Use these tips to help your kids safely use any social media service from networking to image posting sites.

Do you know...

What they're posting?

Check comments and images for personal information, like phone numbers and addresses, as well as inappropriate and illegal content such as hateful or threatening speech and nudity. Delete anything you think is too much information.

How they access social media?

Mobile devices, like cell phones and tablets, let children access social media apps away from adult supervision. Children may post content and even share their locations. Review app settings to help them keep information – like their location – private.

Who they're talking to?

Your child's online contact lists and followers may include people you don't know, or even people your child only knows online. Even if you don't know the contact, make sure you know what images, messages, and other content they're sharing.

What account settings they're using?

This is where you can control who has access to your child's information. Each social media service has a different setup, so take a look at each one your child uses. Always ask yourself – *what* is on the profile and *who* can see it?

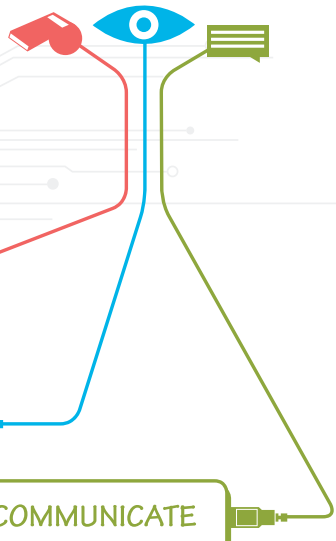
Who has access to their information?

Most social media services have ads and applications from 3rd parties, like games and fan pages. If children click on these or add them to their profiles, they are allowing access to their personal information. Have a discussion about what's OK to add and what's not.

Where to report?

If anyone talks to your child about sex, shares or asks them to share sexual images, or is a victim of sexual exploitation, make a report to the National Center for Missing & Exploited Children® at **www.CyberTipline.com** or **1-800-THE-LOST®**.

PROTECTING YOUR KIDS ONLINE



TAKE CHARGE

Set some ground rules.

Establish basic guidelines like when your kids can go online, what sites they can visit, and how many texts they can send a month, so everyone is on the same page.

Research before you buy.

Did you know that handheld games can connect to the Internet or that many laptops have built-in webcams? Understand what technology you're bringing into your home.

Don't just sit there–REPORT!

If your kids are dealing with cyberbullies or potential predators, report them to the website, cell phone service, law enforcement, or www.cybertipline.com.

MONITOR

Supervise Internet use.

If you can see what your kids are doing, they're less likely to get in trouble.

Safeguards ≠ Safe Kids.

Installing CIA-level monitoring software on your kids' computers does not guarantee they'll be safe online. Technology can't replace your time and attention as a parent or guardian.

Don't go overboard.

It's smart to keep an eye on your kids' social networking profiles, but it's never cool when you post embarrassing messages or pictures to their page.

COMMUNICATE

Talk to your kids; they're not as mysterious as you think.

Your kids might not tell you everything, but that doesn't mean you shouldn't ask. Get involved so you're not the last to know.

Challenge them to a duel.

If you have kids who like to play video or computer games, ask if you can play, too. When you respect their interests, they're more likely to respect your rules.

Don't pull the plug.

Taking away your kids' Internet access because they've done something wrong doesn't solve the problem. Talk to them about protecting themselves and respecting others online.

PARENTS' GUIDE TO SMART PHONE SAFETY

SMART OR SCARY?

Smartphones are essentially little computers, so you might be a little worried when handing one over to your child. Take some time to understand the risks and implement a few safeguards so that you can help your child use smartphones safely.

About 1 in 4 teens report owning a smartphone.

Lenhart, Amanda.
Teens, Smartphones & Texting.
Pew Internet & American Life Project,
March 19, 2012.

THE RISKS

- **CYBERBULLYING**
  With the constant connectivity of smartphones, your child may be more susceptible to cyberbullying or have more opportunities to cyberbully others.
- **GEOLOCATION**
  A GPS-enabled smartphone can reveal your child's location through online posts and uploaded photos.
- **INAPPROPRIATE CONTENT**
  With smartphones, your child has mobile access to content you may consider inappropriate, such as pornography or violent videos.
- **SEXTING**
  Your child may use the Internet and social apps to send, receive, or forward revealing photos.
- **VIRUSES & MALWARE**
  Just like a computer, a smartphone is vulnerable to security attacks if your child accesses unsecured websites and apps.

5 WAYS TO BE SMARTER THAN THE SMARTPHONE!

1. **Be a parent and a resource.**
   Establish clear guidelines, including time limits and consequences for inappropriate behavior, but be open so your child will come to you with any problems.
2. **Set up password protection.**
   This will keep everyone but you and your child from accessing personal information stored on the phone.
3. **Update the operating system.**
   New versions often contain important security fixes.
4. **Approve apps before they are downloaded.**
   Make sure you understand their capabilities and approve their content.
5. **Understand location services.**
   GPS features are useful when using maps, but you'll want to disable location-tagging when your child posts anything online.

Tips:

NetSmartz.org/TipSheets

Gaming Safely

Parental involvement is critical when it comes to helping children game more safely. Take an active interest in the games that your child plays and wants to buy. You can research games' ratings and content on **www.esrb.org**. This website is maintained by the Entertainment Software Rating Board which rates thousands of games each year.

Know which safety features are available on the gaming equipment that your child uses—a headset may have voice-masking features, for example.

Keep gaming consoles in an easy-to-supervise location and be aware of other places where your child may be accessing games.

Tell your child never to give out personal information while gaming or agree to meet anyone outside of the game.

Set rules about how long your child may play, what types of games are appropriate, and who else may participate.

Have your child check with you before using a credit or debit card online.

Check to see if the games your child plays have reporting features or moderators.

Start a discussion with your child

- » Can we play some of your favorite games together?
- » How do you respond if someone bothers you while you are gaming?
- » How much do you let people know about you while gaming?
- » What kinds of people do you game with?
- » Do you feel safe while you are gaming online? Why or why not?

NetSmartz® Workshop
A PROGRAM OF THE
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

CYBERSECURITY MADE CLEAR

While the Internet can make your life easier, it can also expose you to cybersecurity threats like scams and identity theft. Here's what you need to know **before** you go online.

PHARMING
A scheme that sends you to fake websites where hackers secretly collect personal information and passwords.

PHISHING
Fake e-mails that appear to come from a legitimate source looking to "verify" personal or financial information.

TROJANS
Programs that look useful, but actually cause damage to your computer.

SPYWARE
Malicious code that secretly watches what you do on your computer and sends the information over the Internet.

VIRUSES
Self-replicating programs that damage hard drives and affect the normal operation of your computer.

5 Things You Can Do To Protect Yourself & Your Computer

1. **Install firewall**, anti-spyware, and antivirus software, and update them often.
2. **Don't open e-mails** from someone you don't know, download software from a source you don't trust, or enter "free" contests from companies you don't recognize.
3. **Guard your passwords** – don't share them over e-mail or instant message, and change them often.
4. **Type in the website** address instead of clicking on a link.
5. **Look for "https"** or a picture of a lock in your browser window before buying anything or opening an account on a website.