Online Safety Guide for Parents

Definitions, Tools, Tips, and Resources

Technology is changing faster than many of us can keep up with and requires vigilance to stay up to date on the definitions, tools, risks, and resources of the online world. This parent guide covers several online safety topics to better equip parents with the information and resources needed to be "Web aware."Specifically, this resource covers information about netiquette, cell phone safety, filtering, addictive behavior, intellectual property, ergonomics, online privacy, predators, and virus protection. It also includes useful tools to help set guidelines and expectations, such as the Online Safety Contract.

After reading through this parent handout, have a discussion with your family and agree on your own "acceptable use policy" in your household. The Online Safety contract helps guide the discussion and confirm a commitment from the family to follow your household's online rules. Finally, take advantage of the helpful tips and resources to further your investigation of online safety so that you and your family can experience all the benefits of technology and rest assured you have done what you can to be safe in this ever-changing online world.

Netiquette

Netiquette refers to guidelines for acceptable online behavior and communication. Netiquette establishes guidelines that help people communicate effectively, responsibly, and safely.

What Your Child Should Know:

- The responsibility of using the Internet and the school's acceptable use policy.
- When people communicate without seeing the other person's face or hearing their voice, it can be hard to know if they are angry or happy.
- People use different methods like "emoticons" and typing with all capital letters to communicate emotions.
- Messages intended to make your child feel bad are unacceptable. Your child should not reply and should show the message to you or another trusted adult, such as a teacher.
- Online communication should never be used to hurt others by spreading rumors or saying mean things. Never write anything that he or she would not say to someone in person. Your child should tell you or a teacher when someone is trying to hurt someone else.
- Only send or post something a parent or teacher would approve of. Anything sent using technology could be made visible to everyone in the world, and could even be used by someone to hurt your child at any time, now or in the future.

Tips for Parents:

- Create an acceptable use policy for your household that supports the school's policy.
- Discuss news stories regarding right and wrong uses of the Internet.
- Practice writing emails with your child to reinforce and model proper netiquette.

Cell Phone Safety

Cell phone safety focuses on how to prevent and protect a person from potentially harmful situations when it comes to using cell phones and texting. Children should know what appropriate and safe cell phone use looks like.

What Your Child Should Know:

- Do not post phone numbers online, or you can become vulnerable to cyberbullying, criminals who want to meet offline, and scams.
- You can never be 100 percent certain that the person texting is the person who owns the phone. The phone could have been stolen, therefore:
  - Do not text personal information (about himself/herself or others)
  - Never text a password or pin to a friend
  - If someone texts to meet, even if the person is a known friend, call to confirm
- Never let someone you don't know use your cell phone.
- If someone you know needs to use the phone for an emergency or important reason (such as calling a parent), carefully watch what the other person does, to make sure he or she does not impersonate you.
- Ignore unexpected links, files, pictures, and phone numbers, and to only click when it is sent by a known person and your child knows why it was sent.
- Only text or reply to people you know. If the number is unfamiliar, ignore the text.
- Never try to hurt someone or help someone else hurt someone by texting or sending photos.
- Always think about how someone will feel before sending a text. Never text anything he or she would not say in person. If you are angry, stop and wait before texting.
- If someone sends a mean or hurtful message to not reply and show it to you or a teacher before deleting it.
- Anything sent electronically can be forwarded, put online, and used to hurt your child, now or in the future. Online information can remain public for the entire world to see, permanently.

General Phone Usage Safety:

- Never text or talk on a cell phone while driving.
- Excessive texting can cause Texting Teen Tendonitis (TTT), which can lead to Carpal Tunnel Syndrome.

Tips for Parents:

- Use a contract like the Texting Contract in this document to come up with expectations and rules for your child to follow. Come up with reasonable consequences if the contract expectations are not upheld.
- Involve your child in the process of selecting a cell phone and phone plan so he or she understands the costs associated with having a cell phone as well as the features and limitations of the chosen plan.
- Review monthly bills together to stop excessive cell phone use and additional costs for accessing the Internet or buying applications (or "apps") and ringtones.
- Keep an open dialogue about potential harmful situations so he or she has a place to go if he or she feels he or she might be in trouble, or is worried about a situation. Make sure he or she knows you are there for him or her regardless of the offense or situation.
- If you are not a texting expert, ask your kids to teach you how.
- Be watchful and observant of cell phone use. Make sure to talk with your child about negative patterns you see happening before they become worse or potentially harmful.

Filtering

Filters limit where people can go online, and what they can do. They block access to certain sites, or to methods of communication. They can also monitor what kids do online, and control the amount of time they spend there. Many search engines offer filtering options to block any search results parents deem inappropriate.

Options for Filtering Tools:

- Block a person from viewing most sexually explicit material on the Web. But be aware, no filter is perfect.
- Allow parents and caregivers to monitor online activities.
- Allow parents to block out times of the day when a person can or cannot go online.
- Block personal information (e.g., name, home address, etc.) from being posted or e-mailed.
- There are Web browsers for kids that are often designed to be easier to use and automatically filter sexual or otherwise inappropriate words or images.

Tips for Using Filters:

- Have a family discussion and investigate the best types of filters for your family. Create an agreement with your child, setting up guidelines and rules for acceptable computer use.
- Rate filter categories and features based on how important they are to keep your family safe online while keeping the amount of online freedom your child wants.

Addictive Behavior

Addictive behavior has been used to define excessive Internet use. Addictive behavior can be associated with losing the ability to stop going online to the point it impacts other areas of life, including friendships, family relationships, emotional stability, school, and so forth.

Warning Signs:

- The child's school work is affected.
- Friendships and close relationships are neglected or affected negatively.
- The game or online activity is taking up most or all of their leisure time and is preferred over other activities.
- The child becomes angry or displays erratic behavior when he cannot play the game or go online.
- His or her personal space or hygiene is neglected.

Tips for Parents:

- Consider all the factors before labeling your child as displaying addictive behavior.
- Work with him or her to set limits on how much time he or she spends texting, on the phone, and/or computer. Choose a time each day to "unplug" and participate in other activities.
- Investigate software that monitors Internet use. These tools can help remind your child how long he or she has been on the computer so he can learn to monitor and adjust their behavior to begin healthier habits.
- Keep Internet-connected computers in a shared space. When children use a computer in a room shared with other members of the family, they are more likely to self-regulate their use and behavior.
- Monitor your own computer and cell phone use. Your behavior is a model for your child and can serve as a good guideline for responsible technology use.
- Seek help if you see addictive behavior. If your child is displaying addictive behaviors, consider having him or her talk to a counselor. Internet addiction can be symptomatic of other issues, such as depression or anger. Talk to a professional may help to reveal what deeper issues may be spurring the behavior.

Intellectual Property

Intellectual property (IP) refers to creations of the mind – inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. Children come across intellectual property through file sharing and/or peer-to-peer programs, most often in the form of copyright-protected music, movies, videos, or TV shows.

What Your Child Should Know:

- Users of file sharing programs may be in violation of copyright law when they swap or make multiple copies of copyright-protected music, movies, videos, or TV shows.
- Many file sharing and peer-to-peer programs offer access, even accidentally, to illegal images and videos.
- File sharing and peer-to-peer sites can put your computer at risk for allowing others access to your computer, and to malware and "spyware" programs.

Tips for Parents:

- Talk with your child about intellectual property and copyright laws. Make sure they know what is legal.
- Research legal-and-free and/or legal-and-pay options for downloading. Let your child know the options that exist for legally downloading files. Bookmark these sites for easy access.
- Stick to copyright-free MP3s to steer clear of computer viruses and follow the copyright laws. Most file-sharing programs let you choose what kind of files you can search for. Search only for music files (MP3s) and not video or image files.
- Make sure anti-virus software and firewalls are installed and up-to-date on your computer.

Ergonomics

Ergonomics is the study of work. It aims to develop equipment or tools to facilitate work. For children who are on the computer, texting, or playing video games often, ergonomics can be important to their health and safety.

What Your Child Should Know:

- Excessive texting can cause Texting Teen Tendonitis (TTT), the beginning stage of Carpal Tunnel Syndrome.
- Thumb injury can result from the overuse of small keyboards or repetitive motion while playing video games.
- Improper chairs and/or desk height while using the computer can lead to back and neck pain and Carpal Tunnel Syndrome.

Tips for Parents:

- Have your child use a keypad tray and mouse tray. These are designed for better posture and should be set to an angle that keeps the wrists flat.
- Computer chair and desk should be the correct height, support the back, and should not strain the neck.
- Tell your child that too much texting can cause Texting Teen Tendonitis (TTT)
- Explain the symptoms of Carpal Tunnel Syndrome to your child, so he or she is aware of the warning signs..

Online Privacy

Online privacy refers to the way in which we protect ourselves from identity theft and keep personal information safe and secure. Identity theft and identity fraud refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in a way that involves fraud or deception, typically for economic gain.

Online Identity Theft Examples:

- Credit card identity theft – Criminals gain access to credit card numbers and make purchases ruining people's credit for years.
- Social Security Number theft – Online criminals access Social Security numbers to create a new identity or apply for credit. This could damage credit for years.
- Character theft – Someone could use an e-mail address to impersonate and harm others. This type of theft could be damaging to a person's integrity and reputation.

What Your Child Should Know:

- Protecting the identities of family members is a shared responsibility of all family members.
- Never share your Social Security number online.
- Weak passwords can lead to you avatar being stolen or being robbed in online gaming sites.
- Never use personal information like a birth date, Social Security number, or their mother's maiden name as a password or username for any online accounts.
- Do no give out personal information in chat rooms or on social networking sites that allow members to make their addresses and phone numbers public to anyone who views their profile.
- Some sites are secure, but others are not. Always check whether a site's security is authentic before entering any personal information.
    - Use a search engine like Google to get to the site to make sure you typed the Web address correctly
    - Always look for "https:" on any site that asks you to enter sensitive information
    - Look at the URL in the browser, is it the correct site?
    - Never send your username and password or other sensitive information in an email

Tips for Parents:

- Research in the field of online safety has shown that the three behaviors that put youth most at risk online are:
    - Talking about sex
    - Agreeing to meet someone they met online
    - Harassing others online
- You are the first line of defense in protecting your child's online privacy.
- Discuss with your child the importance of personal information.
- Make sure your child leaves only the absolute minimum in personal information on any Web site.
- Bookmark high-quality noncommercial sites for your child that are enjoyable and educational.
- Double-check the settings your child's privacy settings on social networking sites are set so that only friends can see your child's profile. Periodically check the settings since sites may change things over time.
- Shop with your child online. Make sure that any site you use has requirements in place to ensure that transactions are safe and secure. Show your child how encrypted sites use https in the URL address bar instead of http.

Predators

Online predators find children through social networking sites, blogs, chat rooms, instant messaging, email, discussion boards, gaming sites, and other Web sites. They seduce their targets through attention, friendliness, gentleness, and sometimes gifts. They are good at "lending an ear" and sympathizing with children's problems. These predators gradually introduce sexual content into their conversations and may eventually show them sexually explicit material. The biggest threat is that these predators try to find a way to meet the child face-to-face.

According to the Berkman Center Report on Internet Safety, based upon the research done by Wolak, Finkelhor, and Mitchell and M. Ybarra, the children that are at the greatest risk by predators are youth ages 12-17. They are more likely to be female, gay, or questioning their sexual identity. Children who have been previously sexually abused are also at greater risk.

Youth who are targeted inappropriately by adults are often seeking out sexual material or talking about sex online. They have often visited adult-oriented chat rooms where conversations quickly become sexual. Teaching youth to avoid such sites and to present themselves in a non-sexualized manner online is important.

Tips for Parents:

- Talk with your child about online predators and what they set out to do. Explain that most of the people we meet online are friendly but that some individuals may be mean or want to hurt others.
- Talk with your child about healthy relationships.
- Be alert to signs that your child is engaging in inappropriate communications with adults online. Some signs that may occur if your child is a target are:

  - He or she spends a great deal of time online alone.

  - You find pornography or sexual photos on the family computer.

  - He or she gets phone calls from people you do not know, or make calls (sometimes long distance) to numbers you do not recognize.

  - He or she receives mail, gifts, or packages from someone you do not know.

  - He or she withdraws from family and friends, or quickly turns the computer monitor off or changes the screen when an adult enters the room.
  (Adapted from the Web site www.bewebaware.ca/english/sexual_risks_harm.html.)
- Talk with your child about who in his or her circle is considered to be responsible and trusted adults. Discuss other adults he or she can turn to for help, such as teachers, principals, counselors, and coaches.
- Use parental controls software.
- Keep the computer in a common area of the house so it can be seen by others. Sit with your child often while he or she is using the Internet.
- Discuss the importance of open communication and what can happen when your child keeps a secret or withholds information. Explain that no one can tell your child to keep secrets from you, and when they are told to keep secrets from their parents, your child should tell you immediately.
- Give your child tips and ideas for communicating about topics that may be difficult. Use resources such as http://kidshealth.org for tips for kids to start a difficult conversation with parents or another adult.
- Make sure your child keeps his or her number private. Given that so many IM clients now make it possible to send text messages directly to cell phones, never post a cell phone number on any website.
- Make sure your child limits where personal information is posted. Be careful who can access contact information or details about interests, volunteering, or employment to reduce exposure to people he or she does not know. This will protect privacy and reduce unwanted contact from bullies or potential predators.

Virus Protection

Virus protection helps protect a computer against intrusive applications. These intrusive applications include viruses, worms, spyware, and pop-up advertisements. If not protected, a computer can be attacked by harmful applications and data can be destroyed and lost and personal information and passwords stolen.

Types of Intrusive Applications:

- Virus – A virus is a small piece of software that piggybacks on real programs.
- Worm – A worm is a small piece of software that uses computer networks and security holes to copy itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.
- Pop-Up Advertisements – Also known as pop-up ads, these applications open a new browser window. The new ad window appears on top, covering the Web page you want to see. Clicking on the pop-up can sometimes prompt more pop-ups or even worse, contain intrusive applications, like spyware or viruses.
- Spyware – These computer programs truly "spy" on you. Spyware applications sit silently on your computer and intercept personal information like usernames and passwords.

Tips for Parents:

- Install a reliable form of virus protection to help defend against intrusive applications. Without virus protection software, you open yourself and your computer to attacks, identity theft, and computer malware.
- As a family, research and review applications, and choose one to protect your computer.
- Have a family meeting to go over examples of intrusive applications, what they look like, what NOT to do when they pop-up, and what to do when a virus protection program detects an intrusive application.

Resources for Parents

Filtering

- GetNetWise - http://kids.getnetwise.org/tools/tool_result.php3

Intellectual Property

- Media Awareness Network- http://www.media-awareness.ca/english/parents/index.cfm
- World Intellectual Property Organization - www.wipo.int/about-ip/en/

Ergonomics

- Ergoweb- www.ergoweb.com/resources/faq/concepts.cfm

File Sharing

- TopTenREVIEWS - www.internet-filter-review.toptenreviews.com/peer-to-peer-file-sharing.html

Texting

- Connect Safely: www.connectsafely.org
- Scholastic.com: http://www2.scholastic.com/browse/article.jsp?id=3751903

Identity Protection

- KidsHealth: www.kidshealth.org/kid/watch/house/online_id.html
- U.S. Department of Justice: www.justice.gov/criminal/fraud/websites/idtheft.html#whatis

Online Safety

- KidSites: www.kidsites.com
- U.S. Department of Homeland Security: www.us-cert.gov/cas/tips/ST05-002.html

Addictive Behavior

- Be Web Aware: www.bewebaware.ca/english/compulsive_use.html

Our Family's Online Safety Contract

After reading through the parent guide, have a discussion with your family to come to consensus about your own "acceptable use policy" within your household. This contract will help to guide the discussion and confirm a commitment to follow your household's online rules.

Name of Parties: This contract is between _____ and _____.

Statement of Agreement _____

_____

Terms of Agreement

Ergonomics: How will we modify our surroundings to work safely with electronics?

_____

_____

_____

Filtering: What filters are necessary for our family to allow for safe and responsible computer use?

_____

_____

_____

Virus Protection: What kind of virus protection will our family use to protect our computer from intrusive applications?

_____

_____

_____

Cell Phones: What guidelines will we follow while texting and talking on our cell phones?

_____

_____

_____

Online Privacy: What steps will we take to protect our family from identity theft and to keep our personal information protected?

_____

_____

_____

Predators: How will we keep open communication and be proactive about potential dangerous situations and/or predator encounters?

_____

_____

_____

Intellectual Property: What rules and guidelines will we follow to stay within the law when we are using file sharing or peer-to-peer programs?

_____

_____

_____

Netiquette: What kind of acceptable online behavior will our family use to be safe, respectful, and responsible online?

_____

_____

_____

Addictive Behavior: What rules will we all follow to promote healthy technology use? How will we make sure we all follow these rules?

_____

_____

_____

By signing this we agree to abide by and follow the above terms.

Signed _____and _____

Date _____

Texting Contract

Name of Parties: This contract is between _____ and _____.

Statement of Agreement _____

_____

Terms of Agreement

Ergonomics: How will you modify your texting to keep yourself safe?

_____

_____

_____

Prevention: How will you avoid potentially harmful situations?

_____

_____

_____

Safety Actions: Explain what actions you will take to protect yourself.

_____

_____

_____

Social Manners: List the guidelines you will follow while texting.

_____

_____

_____

By signing this I agree to abide by and follow the above terms.

Signed _____and _____

Date _____