Cyber Savvy Parents

The Good News!

Multiple research studies have demonstrated that the vast majority of today's youth are making good choices online and when using cell phones. Most are effectively handling the negative situations that occasionally occur and are not overly distressed by these situations. Most do not like seeing people engage in hurtful online behavior. While from time to time, young people may face situations involving online risk, such risk rarely results in serious harm. Sometimes young people make mistakes that could be prevented if they fully understood the risks and effective strategies to avoid and respond to negative situations.

A minority of young people are at greater risk online. It is important that we continue to pay attention to the concerns faced by these young people.

Cyber Savvy

The objective of parents is to ensure that your child becomes Cyber Savvy. Cyber Savvy young people:

- Keep Themselves Safe. They understand the risks-and they know how to avoid getting into risky situations, to detect whether they are at risk, and to effectively respond.

- Present a Positive Image. They present themselves online as someone who make positive choices.

- Respect Others. They respect the rights, privacy, and property of others and treat others with civility.

- Take Responsibility for the Well-being of Others. They help others and report serious concerns to a responsible adult.

Active and Positive Parenting

Research has found that the children of parents who are actively and positively involved demonstrated fewer online risk behaviors. Further, it has been found that cyberbullied teens whose parents were actively and positively involved were less emotionally distressed and better able to respond effectively to these incidents.

One strategy to be positively engaged with your child about digital activities is this: Every time you interact with your child abut his or her the digital activities, be sure you make one positive statement about your child's good choices. From your child's perspective, interactions with you related to digital activities will "feel good." Thus, your child will be more inclined to want to share aspects of his or her digital life with you.

Through the Years

Guide your approach based on the age of your child:

- When children are young, it is the parents' responsibility to make sure their Internet use is in a safe online environment and that they engage in safe communications. Children who still believe in the tooth fairy cannot be expected to protect themselves online. To them, the Internet is more of a "magic box." Parents must ensure that their use is safe.

- By third grade, young people can begin to grasp essential concepts about how the Internet functions, which provides the ability for them to take on more personal responsibility for good decision making.

- By middle school, many tweens will be able to take on even more personal responsibility for good decision-making. Many tweens want to jump into environments and activities with teens. This shift needs to be made carefully, based on an understanding of your child's social-emotional maturity.

- The most important thing for parents of teens to know is that the "biological imperative" of every teen is to learn to make their own decisions and solve their own problems. It is necessary for your child to learn to independently make safe and responsible choices, which requires practice in doing so. Your important role is to support your child in becoming independent. Obviously, this will involve many "teachable moments."

General Guidance for Parents

These are important general guidelines for parents:

- Appreciate your child's digital activities and digital interactions with friends. Help your child learn to make positive choices in accord with your family's values. *"What a good decision you made ..."*

- Warn against impulsive actions using digital technologies. *"Always remember, anything you send or post can easily become public."* Tell your child that it is especially dangerous to ever send or post anything if he or she is upset or angry--because this is when mistakes are most often made. *"If you are ever really upset, turn off your cell phone--walk away from the computer. Wait until you have calmed down before you do anything."*

- Never overreact if your child reports an online concern. You want your child to feel comfortable reporting such concerns. Your first comment must be positive. *"You are smart to realize this is a problem you should tell me about."* Then indicate a commitment to work in partnership to respond. *"Let's figure out what is happening and work together to find a way to fix this."*

- Use logical consequences. If your child engages in risky, inappropriate, or harmful behavior, impose a logical consequence that will focus your child's attention on why this action has caused or could cause harm to him or her or to someone else. Require that your child remedy any harm. *"What were you thinking? What do you think has happened--or could happen as the result of your actions? How would you feel if someone did this to you? What can you do to make things better?"*

- Pay attention to possible red flags. Red flags include appearing emotionally upset during or after use, disturbed relationships with family members or friends, spending too much time online, engaging in excessively secretive behavior when using digital technologies, and making subtle comments about online concerns. If any red flags are evident, pay closer attention and carefully try to engage your child in discussion.

- Encourage caring for others. Encourage your child to help others directly or report to you or another responsible adult if he or she witnesses someone being harmed or at risk online. *"It is important to make sure everyone is safe online. If you see someone is being hurt or making a bad choice, reach out to help. If the problem is serious, tell me or another adult."*

- Maintain computer security. Make sure you have implemented security against malware, use a spam blocker, block pop-up ads, and use safe search features. Never allow peer-to-peer (P2P) software, as this can lead to accidental access of pornography and is a significant source of identity theft malware.

- Educate yourself on issues of profiling and advertising. Read privacy policies. Point out to your child the strategies sites use to obtain their demographic and interest information and digital advertising strategies, including targeted banner ads, ads integrated into games, and sites that ask people to sign up to receive ads. Take advantage of the emerging ability to restrict the ability of sites to track your child's activities for profiling.

Tips for Parents of Children

These are recommended strategies for parents of children:

- Create a "fenced play yard" for your younger child online. Limit your child's access to sites you have selected as appropriate. As your child grows, make these decisions together. Look for family safety features that allow parents to limit their child's access to selected sites, control who can communicate privately, manage time spent online, and review the history file. You can also create a "fenced play yard" using bookmarking and a combined parent/child email address.

- Make sure you personally know everyone your child communicates with through e-mail, instant messaging (IM), and any other form of personal communications. Limit communication with strangers to general areas of safe, moderated children's sites.

- Help your child create a safe and fun username that does not disclose personal details, as well as a safe password. Make sure your child knows to never disclose his or her password to anyone other than you. Use your e-mail address for any site registrations.

- Keep your family computer in a public place in your house so you can remain engaged in what your child is doing. Your child should know that everything he or she does online is open to your review.

- If you provide a cell phone to your child, implement the safety and security features provided by the company.

- If you want to allow your child to participate in a social networking environment, select a safe site that is designed for children, not for those over 13.

Cyber Safe Kids

Your child should understand these safety guidelines:

- *Keep Yourself Safe. "Stay on the kid's sites that are safe and fun. If you want to go to a new site, tell me, and we will check it out together."*

- *Keep Your Life in Balance. "Keep the time you spend using technologies in balance with other fun activities. (In other words, "Enough screen time, go outside and play, go read a book, let's call a friend.")*

- *Think Before You Post. "Post material that shows people you make good choices. Never post your address or phone number."*

- *Connect Safely. "Communicate only with friends you know and trust through email or personal messaging. Communicate with strangers only the safe kid's sites we have found."*

- *Stay Out of the Garbage. "If 'yucky' stuff appears on your computer, turn off the screen, like this, and tell me."*

- *Spot the Ads. "Make sure you can tell the difference between fun activities and ads for kid's stuff."*

- *Be Kind Online. "Treat others kindly online. Before you send a message or post material about someone else, think about how you would feel if someone sent you that kind of message or posted something like that about you. If you receive a hurtful message, ask me for help so we can figure out how best to respond."*

Tips for Parents of Tweens & Teens

These general guidelines are recommended:

- Tweens and teens will not stay in "electronically fenced play yards." (Conduct, a search on the term "bypass Internet filter.") The new marketing push is for parents to install monitoring software. Most teens would view this degree of intrusiveness as an indication of lack of trust. Use of monitoring might be an appropriate logical consequence if your child's use of technologies has been highly inappropriate.

- Pay attention to what your child is doing online, but balance your supervision with your child's emerging legitimate interests in personal privacy. Remember, if your child feels you are overly intrusive, it is exceptionally easy to find a way to go behind your back. Positive interactions, both face-to-face and online, will be more effective in encouraging your child to share.

- Implement the use of cell phone safety and security features provided by your cell phone provider that are appropriate to your child's age and demonstration of personal responsibility. Discuss issues of responsible cell phone use, including responsible texting and issues around the capture or sending of images. Show your child how easy it is for anyone to forward or post something they have sent digitally. Make sure your child turns off his or her cell phone when going to bed. If there are any problems associated with this, use the security features that allow you to control time of use.

Many tweens and almost all teens are actively engaged in social networking. These guidelines are recommended

- It is best not to allow tweens to register on social networking sites for users over the age of thirteen. Make this decision based on your child's maturity.

- When you decide to allow your child to start social networking, go through all privacy settings with your child to make sure that only accepted friends can see your child's profile.

- Insist that your child only establish friendship links with people whom he or she knows and trusts, and review all friends to make sure this is the case. As your child gains experience in social networking, allow your child more freedom to exercise his or her own good choices. This includes the establishment of friendship links with people whom your child's friends know face-to-face.

- If your child is younger, or has a habit of not making good choices, it is likely best that you have your child's login password, so you can review everything that is happening. For most children, the best way to supervise is to create your own profile and friend your child. This way you can regularly review what is happening, including materials posted and friends added.

- Advise your child that you will regularly review his or her profile, and if any material is posted that is not safe or not in accord with your family's values, you will place restrictions on his or her use. As your child gains experience and demonstrates good decision-making, you can back off this review.

Cyber Savvy Tweens & Teens

The following are the guidelines for tweens and teens to be Cyber Savvy:

- *Avoid the Impulse. Remember, What You Do Reflects On You.* Engage in effective problem solving and positive decision making before posting or sending anything digitally. Be a helpful ally if you see someone is at risk or is being harmed.

- *Read With Your Eyes Open. Assess the Credibility of Information and Trustworthiness of People.* Carefully assess the credibility of information and the trustworthiness of people by considering issues such as how important it is to make sure the information is credible or person is safe, watching for evidence of bias or attempts to manipulate, and by asking the opinion of others.

- *Keep Your Life in Balance. Avoid Addictive Use of Digital Technologies.* Ensure your use of digital technologies does not interfere with other activities that make your life happy and successful.

- *Think Before You Post. Protect Your Reputation and Respect Others.* Recognize that whenever you post or send material in digitally it can be widely distributed and affect your reputation—positively or negatively. Respect the rights and privacy of others.

- *Connect Safely. Interact Safely With Others Online.* Be careful when you interact with people online. Only let people you know, or those whom your good friends know, have access to your personal profile. If you want to meet in person with someone you have gotten to know online, make a safe meeting plan in a public place and bring along friends.

- *Keep Yourself Secure. Implement Security and Avoid Scams.* Ensure your computer security is maintained and your activities do not increase your risk. Do not share your password. Watch out for scams—offers that are too good to be true or threaten loss if you do not share personal information.

- *Abide by the Terms. Act in Accord with Policies, Terms, and Laws.* Follow the common standards to protect the rights of everyone.

- Stay Out of the Garbage. Avoid Objectionable and Illegal Material. Use safe surfing techniques to avoid accidentally accessing garbage. Know how to effectively respond if such material is accidentally accessed. Don't access or distribute illegal child pornography.

- *Don't Sell Yourself. Disclose and Consume Wisely.* Make a personal decision about how much personal information you want to share with sites and apps. Use the Internet to research companies, products, and services before you make purchases.

- *Protect Your Face and Friends. Be Savvy and Civil When Networking.* Protect your privacy by limiting access to your profile only to those you have friended. Protect your reputation and respect others when you post. Friend only people whom you, or a trusted friend, know in person. Report abuse.

- *Embrace Civility. Prevent Hurtful Digital Communications.* Exercise care when posting or sending material so you do not place yourself at risk of attack. If someone is being unkind, wait until you have calmed down to respond. Save the evidence. Then calmly tell the person to stop, ignore or block the communications, or file an abuse report—or all three. If the person does not stop, ask for help. Recognize that no one deserves to be attacked online. If you hurt others, this will damage your reputation and friendships. If you see someone being harmed, provide support to that person and speak up against the harm. If the situation is serious or continues, report to a responsible adult.

- *Cyberdate Safely. Avoid Exploitation and Abusive Relationships.* Proceed with caution when forming a relationship through digital communications—watch out for "fantasy" relationships. Don't let someone exploit you—if someone appears to be trying to manipulate you to engage in sexual activities or requests a nude photo, discontinue contact and report this to an adult. Do not allow a partner to control and abuse you using digital technologies.
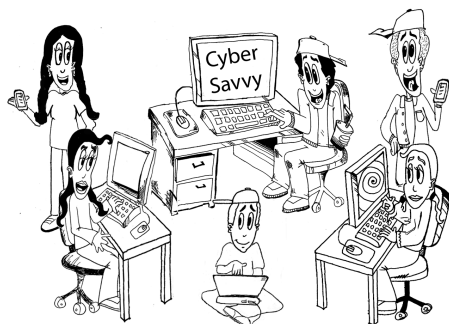
Embrace Civility in the Digital Age

Embrace Civility in the Digital Age (a program of Center for Safe and Responsible Internet Use) promotes approaches that will best ensure all young people become cyber savvy and that seek to address youth risk in the digital age in a positive and restorative manner. Web site: http://embracecivility.org E-mail: info@embracecivility.org