Tech Safety Checklist

The following list is designed to assist parents to think and talk through important technology safety concerns with their children. You can use the check boxes to mark off the different topics as you discuss them.

- **Keep private information out of the public eye**:

Teens often innocently reveal information that would let dangerous people find their real-world location. Pay particular attention to your teen's online profile. This is a component of a social networking site that allows teens to potentially share too much of their contact information. A social networking site may even prompt teens to enter their full name, address, school name, birthday, names of family members, email address, cell phone number, and more when setting up their profile for the first time. Make it clear to your teen that they do not have to (and should not) supply personal information just because it is suggested they do so.

- **Parental Controls**:

Parental Controls can help you be in charge of what your kids are doing online. Parental Controls are available on many gaming systems, websites, and mobile phones. Visit your gaming system or cell phone carrier's web site and search for parental controls to learn about your options.

It is worth noting that the Microsoft Windows 7 operating system offers many free parental controls such as:

1. Web Restrictions – allows a parent to restrict what types of web sites their child can visit, either by category (eg. My child cannot go to pornographic sites, or gambling sites), or specific URL to determine what sites are allowed and which are not. These restrictions will work automatically with any web browser.
2. Game Restrictions – Partnering with Computer Game rating systems from around the world, Windows 7 allows a parent to restrict the types of computer games that their child can play.
3. Application Restrictions – If a parent chooses, they can apply limits so their child can only run applications that the parent has approved.
4. Time Limits - Parents can decide when children are allowed, or not allowed, to use the computer by choosing the specific times and days to block. The child then receives a 15-minute and a 1-minute notification that their time is about to expire, and if their time ends before they log off the computer, Windows 7 suspends their session and displays the logon screen so another user can use the computer. The child's session stays active in the background, however, so the next time they log on, they can pick up where they left off without losing any of their work

- **Blogs and Twitter:**

If your teen has their own blog or uses Twitter, be very careful about what they share about themselves and your family. Consider asking your teen to give everyone a nickname instead of using their given names to protect your privacy. For example, if your teen wants to describe an activity she did with her little sister, it may be wise to refer to the sister as Lil Sis instead of as Beth. Set the privacy settings on the blog to keep strangers out. Discourage your teen from providing current updates of their location since doing so makes it too easy for someone to find them wherever they are.

- **YouTube**:

If your teen creates videos and posts them on YouTube, they can and should restrict public access to the videos they post (go to Edit Your Video and select Broadcast Options). Never allow your child to publicize their full name and contact information when posting a video. If you are concerned about the types of videos your child may be exposed to when using YouTube, you will be glad to know that the program has a safety mode. While it doesn’t block all offensive content, it does block some. Activate it by go to YouTube.com and clicking on Safety Mode at the bottom of the screen.

- **Teenage Hacking**

1. Have you told your kids that hacking and violating people’s privacy is not a joke?
2. Have you warned your kids that their online passwords are private and should stay that way?

- **Formspring:**

Some teens have embraced a newer social networking site called Formspring that is based on a question/answer format. Users can anonymously ask questions that they would never ask in person. The questions can range from the benign: "Are you going to the movies tonight?" to the more sexually driven: "What size are your boobs?" to pure hate mail: "You stink and no one likes you."

1. Does your child use Formspring?
2. Does your child know that they can block questions submitted anonymously?
3. Is Formspring worth using?

- **Online Reputations**:

If you post it to the web, be prepared for anyone and everyone to see it:

You never know when a college admissions officer or prospective employers might search for you online. If they find you, what information about you will they see?

1. Remind your children that all private information can be made public. Posts on a friend's wall, private text messages, intimate photos, and emailed jokes can all be cut, pasted and sent around.
2. Emphasize that whatever they post online will persist long after they have removed it.
3. Insist on the highest standards of courtesy and decorum: – no bullying, no coarse language, no inappropriate photos or hobbies (like under-age drinking or smoking)
4. Remind your teens that anything they post can be misused by someone else.
5. Do not engage in flame wars by posting hateful messages back and forth.
6. Set family computer use guidelines.

- **Misleading and False Information.**

You can help protect your children from being deceived by false content by:

1. Informing them that just because something is on the Internet, that doesn't automatically make it true.
2. Explaining that there is no overriding organization deciding what should be on the Web or taking responsibility for its accuracy.
3. Encouraging your kids to be suspicious of things that seem unlikely or improbable
4. Making yourself available to answer their questions.
5. Introducing them to Snopes.com so they can check out the veracity of pop culture ideas and urban myths

- **Pornography.**

You can help protect your children from viewing pornography by:

1. Making it clear that it is not appropriate for minors to view adult content.
2. Obtaining protective software for your computer to make it more difficult for your children to access such materials.
3. Creating a plan for what your kids should do if they stumble into a sexual website
4. Checking your computer to see if your kids have visited pornographic sites or downloaded x-rated images (for help with this, see Check Your Computer's History in this section of the program).

- **Texting and Sexting:**

1. Make sure your kids are using their mobile devices and cell phones appropriately. This means, no rude or intimate texts or pictures.
2. For younger kids, monitor the texts they are sending and receiving.
3. Monitor the time of day that your child is texting and making calls. Decide if you want to set up a guideline on when your child can have their phone with them and if they should keep it in a public area of the home during the night.
4. Emphasize with your kids that sexting at any time is not appropriate. Kids will often say something as a joke or that they think is only between close-friends, but with texting and online messaging, messages can be forwarded very quickly.
5. Talk with your kids about what to do if they receive a sexually explicit message. They should not post or store any inappropriate photos of anyone under 18. Any association with pictures of this nature can be considered criminal. Your child could be charged with possession, production or distribution of child pornography.
6. Distribution of intimate pictures of your child could lead to them being the subject to jokes, bullying, blackmail, expulsion from school and loss of a job. These images can circulate forever and never be completely erased.
7. Visit thatsnotcool.com with your child to discuss the content and educational materials that help your child understand the consequences of sexting.

- **Hijacked websites**.

You can help your children avoid accidentally going to the wrong website by:

1. Suggesting that they use a search site or engine like Google or when they are looking for information instead of guessing at the Web address.
2. Investing in filtering software, monitoring software, and home firewalls

- **Web cams**

1. Find out if your kids have a webcams and learn how to tell if the camera is turned on or off.
2. Have discussions about what types of digital images are appropriate for sharing and which are to be kept private.
3. Find out if they use Skype and make sure they are using it in safe ways.
4. Tell your kids that video chats like Chatroulette are off limits to them because of obscene content.

- **CyberBullying**

1. Help your kids develop empathy, self-awareness, and effective decision-making by asking them to always consider:
2. Am I being kind and showing respect in my online interactions?
3. How would I feel if I or a good friend were treated the way I am treating others online?
4. What would a trusted adult think of my online behavior?
5. How would I feel if others could see me?
6. Tell your kids to report online threats or distressing material to you, the school, school violence or suicide hotline, or the police. They shouldn't retaliate or respond to any threatening messages. They should block the bullies immediately and tell someone they trust. Ask them to save the files. Ensure them you will never blame them or remove their cell phone or computer access privileges for reporting what they see.
7. Monitor what your children are positing and check their mobile messages. If your kid is doing the bullying, establish strict consequences and stick to them**.** That goes for mean or sexual comments about teachers, friends, and relatives.
8. Educate your child that forwarding mean messages or just standing by and doing nothing empowers bullies and hurts victims even more. If you can, tell bullies to stop, or let them know bullying is not cool - it's cruel abuse of fellow human beings. If you can't stop the bully, at least try to help the victim and report the behavior.
9. Be aware of signs that your child might be bullied: fatigue, difficulty focusing, sadness, anxiety, anger or fear; avoidance of friends, school, activities; decline in grades; personality changes. Be extra vigilant if he or she has traits that make them stand out, such as obesity, the perception they are gay or lesbian, being an alternative thinker, being unwilling to play social games or sports, and either desperately wanting to be in the "in crowd," or just the opposite—hating the in-crowd.

- **Online Gaming.**

You can help protect your kids from violence related to video gaming by:

1. Familiarizing yourself with the video game rating system and deciding what level of game is appropriate for your child (GetGameSmart.com).
2. Helping your child choose a username that won't invite harassment from other players.
3. Making it a rule that your kids can play games with "friends only" since sometimes other gamers can trace their computer's ISP address to find them in real life.
4. Discouraging "trash talk" between players via Instant Messaging during game sessions which could lead to problems.
5. Obtaining software to help monitor and filter your children's Web activity.
6. Setting parental controls on gaming consoles, especially those with the capability to go online (Nintendo.com, Xbox.com, Wii.com).

- **General web safety**

1. Set a limit on the number of hours your kids can spend online.
2. Impose a computer “curfew,” at which time all digital communication has to cease.
3. If your child is typing or texting in shorthand (OMG, AITR, 9) visit Netlingo.com to learn what their acronyms mean.
4. If your child visits chat rooms or uses Instant Messaging, encourage them to use gender-neutral screen names like BigCheese.
5. Explain what cyber-stalkers are and how they operate. Come up with a plan for what you want your child to do if he or she thinks they have met a cyber-stalker online
6. Instruct them never to open an attachment or click on a link in an email or message sent to them by a stranger.
7. Also explain that ?lling out registration forms and entering online contests is sometimes a means for disreputable people to obtain their contact information.

- **Online Shopping.**

You can help protect your kids when they shop online by:

1. Asking them to get your permission before making an online purchase
2. Insisting that they only deal with reputable merchants who encrypt your personal data
3. Warning them not to purchase items for sale in pop-up ads or Spam emails
4. Paying only with a credit card or with PayPal.
5. Saving copies of your order confirmations and transaction details.
6. Installing Internet safety software on your computer and using an updated web browser when you shop
7. Reviewing all your financial records regularly to make sure there are no unauthorized charges.
8. Checking the computer to see if your teen is visiting gambling sites

- **Illegal File Sharing**

1. Know what kind of music and files your child is downloading. Know the devices they are using (mp3, ipod, computer).
2. Make some rules about where your child can download files from and where they can save it to.
3. Inform your child that downloading media files over the Internet and sharing them with friends can be illegal.
4. MusicUnited is a useful resource to help find digital music that can be legally downloaded
5. RespectCopyrights.org maintains a list of sites where you can download and watch movies legally.

- **Technology Etiquette:**

1. Unless it is an emergency, do not make and receive calls or text messages while dining, riding in a vehicle or plane, or at the movies, job, museum, school, or place of worship. Excuse yourself and walk away if you have to communicate with your phone and silence your ringer in these places too.
2. Never use the phone while driving unless you have a hands-free accessory.
3. Never text while driving!
4. If you are having an in-person live conversation with friends, try not to take non-urgent phone calls during your visit (unless it is your parents calling).
5. Pause your iPod and take out both earbuds when an adult is speaking to you.
6. Don’t send texts or make phone calls late at night and be considerate how many times you text your friends each day (sending too many texts can seem like harassment).

- **Netiquette:**

1. Respond promptly to emails from respected adults like bosses, teachers, parents, family members, and college recruiters.
2. Use the subject line in an email to alert the recipient about what your email is about
3. Before you send your friends a lot of forwarded mail, find out if they really are interested in reading what you have to share.
4. When sending a mass email, use address book functions that protect the privacy of the recipients while not burdening your reader with having to scroll down past rows of email addresses just to get to the message (bling carbon copy).
5. If you are not ready to respond to an email you have received, at least confirm that you received it and let the sender know when you will have a full reply for them.
6. Don’t plagiarize materials that others have created, passing them off as your own work.