Message to Parents and Caregivers about Internet Safety

Digital technology and internet access is now a way of life for most people and for all young people. Your child has received information on how to use the internet and technology in a safer and more respectful manner but parents and caregivers also need this information in order to properly supervise technology use.

This summary has been prepared for you so that you will know what your child has been taught. Without parental involvement many children will be a victim of their natural curiosity and will get into trouble when using technology. I have provided links at the end of this document that you can use to continue your learning process.

Access. You have given your child devices that enable them to access a very powerful and largely unregulated source of information. Access to the internet and social networking sites can be a very positive experience but it can also expose your child to negative experiences. As a caregiver and as the owner of the technology you need to be involved in your child's internet experience. You need to understand what they are doing online and the applications (app or apps) that they are using. Many applications such as Facebook and Instagram require members to be at least thirteen years old. If you have children younger than thirteen years using any of these services you should cancel their membership until they reach the appropriate age. The restrictions are in place for a reason. You need to know who your children are talking to, who is talking to them and what they are saying. Unfortunately, there are many online predators that use the internet to access our personal information and to get closer to us for all the wrong reasons. These predators will often use deceit, trickery and malicious software to achieve their goals. They can access us from anywhere in the world. Many parents give their kids a phone in case of an emergency but be careful to not create a different kind of

emergency by not knowing what they are doing with their phones. Technology should not be used as a baby sitter.

Remember, it is your phone, not theirs. You signed up. You probably bought it and you probably pay the bill. Anything your child does with that phone, either through texting or on the internet (if you have a data plan), will ultimately affect you, because it is your name on the account. You need to create an understanding with your child that you will have full access to their phone and computers. They must give you all their passwords and explain all of the apps and programs they are using. You should be able to recognize all the symbols on your child's devices and know what type of app they link to. The younger the child, the more access you should have. You can give more freedom and responsibility to your child as they age and as your trust level increases.

Malware. Malware are software or programs designed to give a criminal access to your computer. This type of software is usually introduced into our devices when we visit an unknown or untrustworthy web site or by opening attachments in emails from unsolicited sources. Online criminals will also use fake websites to trick us into revealing our personal information. All of the computer applications we use have weaknesses and these criminals will use these weaknesses and malware to achieve their goals. Once malware is installed on your computer other people can have access to your files, pictures and passwords, etc. They may also be able to see all your keystrokes, turn on the webcam or install other malware on your computer. It is important to install anti-virus software and a firewall on your devices to block these types of files. You also need to be careful when opening attachments sent to you via email.

Personal Information. The services provided to us on the internet may be useful to us but they are designed to collect our information. That is how the designers of the software make money. Services

like Facebook, Instagram, Skype and Snapchat all collect our information and sell it so we can be marketed to. When your child takes a picture and they send it to a friend much more than the picture is sent. Information on the time, date, location, who called who and the length of the call are also collected, stored and sold to marketing companies. In order to avoid some of this data collection you can turn off the geo-locating function on their smartphones. This is GPS technology installed on all devices. Look to your manufacturer's instruction manual or search the internet for instruction on how to do this. We are also prone to providing information about ourselves. Instill in your child the importance of not providing too much personal information when using technology, as that information could become available to criminals if they gain access to their devices. Your children should be cautious about whom they interact with online and should be suspicious about becoming "friends "or chatting with people they have not met in person. All social networking sites have privacy settings that can change frequently. Many sites have user agreements that allow the developer to change the privacy settings without informing you and if you click "agree" to the terms you are accepting this right to change the settings. It is for this reason you should check the settings often and you should maintain the privacy settings at the most private, at all times, in order to provide the maximum protection for your child.

Social Networking. There are many social networks that are available today. Many have age restrictions that state users must be at least 13 years old. As a caregiver, you should know what social networking sites your child is using and if they are old enough to be a member of the site. Some of the more popular sites being used these days are Snapchat, Ask.fm, Kik, Facebook, Twitter and Instagram. Although there are many positives to using these sites they are also places where bullying occurs and online predators can gain access to your children.

Know the sites your children are using and monitor their activity to ensure their safety.

Wifi. Wifi is wireless internet access. You should never use public wifi hotspots to do any financial transactions. Anyone can create a wifi hotspot with their internet enabled device and use it to intercept your data. If you have wifi at home, change the password given to you by the manufacturer as many of these passwords are available online and can be used to hack into your wifi account. Hackers could use the internet at your expense to download unwanted or illegal files.

Online Bullying. If your child is being bullied, ask yourself if access to technology is making the situation worse. If your child is being bullied online you should cease all contact with the bully, save the details of the contact or print it off for your reference. Contact your internet service provider and your child's school to report the activity and inform the police if you believe a crime is being committed. For instance, the police would be interested in things like repeated unwanted contact, threats, impersonation of your child and any hint of inappropriate contact from an adult.

If you are unsure if your child is a victim of bullying, look for changes in his or her routine. Bullied children often become more withdrawn, check their devices obsessively and may exhibit a loss of appetite. They may also suffer from lack of sleep, missed days of school and any other new negative behavior. Have a conversation to try to find out what is happening.

Ask yourself if you think your child may be involved in bullying behavior. Aside from being cruel and insensitive, if a child is allowed to continue to bully they could bring civil action to your household, they could be suspended from school and/or the police could charge them with a criminal offense.

Passwords. You and your children need to have long passwords for all your devices and the applications you use. A series of random words that are easy for you to recall works best and password testing sites show you get the best results at about 14 characters. A good example of one would be (ToLiveandDie!) Without the exclamation mark the password would take 3000 years to crack but with

the exclamation mark it goes up to 4,000,000 years. That last digit makes a big difference. Passwords should be changed regularly, or if you suspect they have been compromised. Work out a system to keep track of your passwords so that you maintain access to your accounts but not weaken your security. Websites such as LastPass and Keepass enable you store all your passwords in a secure location without writing them down. This way you only have to remember one strong password.

Top ten Things to Consider

. Don't allow your child unsupervised access to the internet. Keep the computer in a public area of the home and don't allow devices in the bedroom

. Maintain open access to your child's devices so you can monitor their activity

. Keep your child off social networking sites until they reach an appropriate age

. Review all family members' profiles and remove excessive personal information

. Delete fake friends and lockdown the security on all your social networking sites

. Use strong passwords that incorporate upper and lower case letters, numbers and special characters

. Use antivirus programs and a firewall on your computer

. Allow automatic updates to all programs you use to ensure they are best equipped to block unwanted files

. Be suspicious of unwanted emails and requests for information

. Review the links provided and stay current with the technology you use

Some Resources and helpful links

http://computercrimeinfo.com/

FBI computer Crime Specialist

http://keepass.info/

Password Storage

https://lastpass.com/

Password Storage

http://www.youtube.com/watch?v=bE1gj6sNU-U

netnanny

http://www.youtube.com/watch?v=L2VrwQyeNOY

McAfee Safe Eyes

http://www.youtube.com/watch?v=ZL1NoI0qJVg

McAfee Total Protection

http://www.youtube.com/watch?v=Ykx_vWMKLOA

McAfee Parental Controls

http://www.pcmag.com/article2/0,2817,2407509,00.asp

Smartphone Apps

http://windows.microsoft.com/en-CA/windows7/products/features/parental-controls

Windows Parental Control

http://en.wikipedia.org/wiki/Parental_controls

Parental Controls Wiki

http://www.rcmp-grc.gc.ca/is-si/index-eng.htm

Cyber Safety

http://www.staysafeonline.org/stay-safe-online/

Cyber Safety

http://www.netlingo.com/

List of Texting Shortcuts

http://www.consumer.equifax.ca/partnerca/maclt/free_en.html?gclid=CI-FvabZmr4CFchFMgod_2cARQ

Check your credit

http://www.cyberbullying.ca/

Anti-bullying site

http://www.bbb.org/council/bbb-scam-stopper/

Scams

http://www.pcmag.com/article2/0,2817,2403388,00.asp

Virtual Private Networks

https://en.wikipedia.org/wiki/Two-factor_authentication

Two Factor Authentication

https://technet.microsoft.com/en-us/magazine/2008.05.desktopfiles.aspx

Non-administrator Account