SCHOOL COUNCIL INTERNET SAFETY GUIDE

ROCKWOOD CENTENNIAL PUBLIC SCHOOL

137 Pasmore Street, Rockwood, Ontario N0B 2K0

Phone: 519-856-9556 Fax: 519-856-9563

K. Creery, Principal W. McGee, Office Co-ordinator

S. Marquis, Vice-Principal Web site: www.ugdsb.on.ca/Rockwood

June 2011

Dear Parents,

In May, Rockwood Centennial School Council hosted a seminar on ***Social Networking and Internet Safety***, highlighting both the online benefits and the potential risks to children. **Detective Paul Krawczyk of Toronto Police Services, Child Exploitation Unit,** highlighted how it could be a particularly tough social landscape to navigate for kids already dealing with poor self-esteem, including Facebook depression, cyberbullying, sexting, child pornography, luring and other online risks. As a follow up to this enlightening, yet disturbing evening, Kevin Hadley of Click Computer Services, has created this guide for parents as a tool to help keep you and your children safe online. For a more personalized approach to securing your computer we invite you to contact Kevin Hadley directly at Kevin@click360.ca.

Sincerely,

Caroline Mills, Chair Lynn Clack, Treasurer

INTERNET SAFETY FOR KIDS AND FAMILIES

The Internet is now an integral part of everyday life. Within a short period of time, it has evolved from being a tool for accessing information and conducting communication and commerce to becoming a significant venue for social activity and interaction. For many young people who have never known a world without the Internet, it is also a vehicle for self-expression, a source of entertainment, and a creativity and distribution tool unimaginable for previous generations.

Know the risks

The Internet should be a place where kids have fun communicating with friends and learning about the world around them. While using the Internet is an integral part of a young person's life and a necessary life skill, there are risks associated with it. This guide will help parents become aware of these risks and to avoid or minimize their impact, keeping children's online time constructive.

In general, the positive impact and benefits of the Internet outweigh its risks. In considering the risks, it is important to take into account what may reach young people through the Internet as well as what they may share over the Internet with the outside world. Not all young people will encounter all of the potential hazards listed below, but by being aware of them, families can consider how to respond to them before ever going online.

What may reach them

Inappropriate content
Unwanted contact
Aggressive or undesired commercialism
Covert web threats

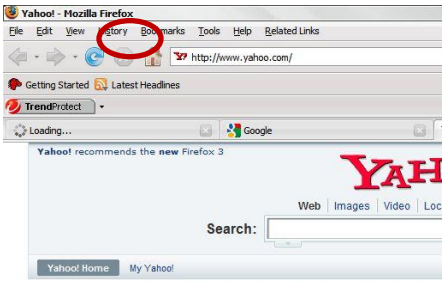
What they share with the world

Personal/private information
Disparaging comments about others
Unintended and/or illegal file-sharing

Below are some additional safety measures you and your child can do together particularly if your children are just beginning to explore the Internet:

1. Keep computer in a common area.
2. Agree to time limits for Internet use and all social devices - cell phones, Nintendo DS, ipods, PS2, Xbox, Playstation 3.
3. Keep software security up-to-date, some examples are *Trendmicro, Norton, AVG, or EST, etc.*
4. Agree on websites your kids can visit (for younger children).
5. Use URL filtering. URL filtering is a means to control or "filter" content. This includes setting parental controls within your security software or your browser settings *(Internet Explorer, Safari, Firefox etc).*
6. Download a website reputation service. *An example is http://safeweb.norton.com/*
7. Review the content and the privacy and security policies of the sites your child frequents.
8. Speak with your kids about entering personal information online.
9. Encourage them to ignore unwanted contact from people they have never met.
10. Run a manual scan with your software security – located at the bottom left of your computer screen.

11. Check browser history. Most browsers will have a History button in the top toolbar. Generally if a family uses the Internet frequently and there is no history, it may have been intentionally deleted.



Be prepared for what they might share

In general, using common sense and critical thinking are a strong foundation for a young person to stay safe online. Any interactions they have on the Internet should be done with the same approach as they would offline, so talk to your kids about using the guidelines below whenever they are online.

1. Be cautious & wise about what you post. ***Only post online what you would comfortably share with your entire class.***
2. Set profiles on social-networking sites to private. ***With Facebook click on the settings option and customize the account settings.***
3. Use nicknames, not your real name, to identify yourself.
4. Be respectful of others.
5. Use legal file-sharing services only. ***For example, using iTunes for legal music downloading.***

SAFETY TIPS FOR SOCIAL NETWORKING

As a social medium, the Internet enables young people to stay in touch with friends when they are physically separated and sometimes to meet new people who share their interests. Social networking sites, chat rooms, message boards, and blogs are some of the many ways this is possible on the Internet.

Know the risks

If a young person is socially active on the Internet, he or she is very likely managing at least one personal profile on one or more social-networking sites which require or allow them to publicly divulge something about themselves, including Facebook, form spring, Twitter etc. While this ability is not inherently bad, there may be people familiar or unfamiliar to them who could take advantage of this.

Unwanted contact

Behaviors such as online grooming *(technique used by a sexual predator to convince an underage person to have relations with them offline)* and cyberbullying *(online harassment of classmates or peers)* are some examples of unwanted online contact that parents and care-givers should understand and help young people recognize and act on if they ever experience it. In both cases, the first and best response is to encourage kids not to respond to such messages and to alert their parents so they can figure out the next steps together. It is also a good idea not to delete the messages in case they later need to be used as evidence.

Aggressive commercialism

In addition to unwanted contact, parents and caregivers should be mindful of online messages - sometimes legitimate, sometimes malicious - that entice young people to acquire products or services in exchange for information or money. It is important to be aware of how this type of commercialism is delivered, what is being offered, and what young people may do as a result. Vendors are using more creative ways to promote their goods and embed their marketing messages, which may make it difficult for a young person to differentiate between an advertisement and the content they are accessing or even interacting with (a technique called immersive advertising). Free offers and promotions for age-inappropriate products and services (dating services, gambling services, etc.) may also be compelling enough to a young person to enter personal information that could later be used by the advertiser to deliver continuous, intrusive advertising (spam or pop-up advertising) or worse, perpetrate cybercrime (hack attacks, identity theft, etc.).

Covert web threats

Social networking sites are also an increasingly popular place for cybercriminals to deceive people into divulging information or downloading software onto their computers for any number of uses. Their methods range from simple to elaborate. Sometimes a young person will see an advertisement or link to download seemingly harmless software that they can use on their own social networking profiles, such as a widget – programming code, but which in fact has been infected with malicious software that gets downloaded along with the legitimate software. One example is the Facebook "Secret Crush" widget, reported in early 2008 by Fortinet as luring users to install Zango adware.

Some applications that run on social networking sites may encourage young people to complete a survey or provide information that might not be appropriate to share with others. Other times, a young person can be lured to see an "attractive" video but is told it is necessary to download a viewer in order to see it. While downloading a viewer is a normal action necessary to see videos online, the viewer could be infected with other software that, once installed, can be used by the cybercriminal to steal information from the computer, spy on the activities of its owner, or other uses depending on the type of malicious software installed.

Behaviors toward others

The anonymity of the Internet can unfortunately encourage offline bad behavior to continue and be exacerbated online. Young people can be victims as well as participants in behaviors such as cyberbullying and harassment**. It is important to know that information they post can be accessed by anyone virtually forever and can potentially be traced back to them, so it is best to be respectful of others, online or off.** More severe comments, particularly those involving physical threats, may also be considered a criminal offense.

Below are some guidelines for young people to follow when they are using social networking sites, chat rooms, blogs, or message boards:

1. Use a nick name or code name.
2. Set your profiles to private.
3. Keep personal information to yourself – only post information online that you would share comfortably with your entire class.
5. Keep your security software up-to-date. Most systems send reminders as to expiration dates.
7. Avoid in-person meetings.
8. Be nice online.
9. Think about how you respond.

Below are some guidelines for parents to consider when allowing kids use social networking sites, chat rooms, blogs, or message boards:

1. Try to set reasonable expectations.
2. Speak with your kids about how they use the services.
3. Support critical thinking and civil behavior.
4. Consider requiring Internet use in a high-traffic place in your home.
5. Try to get your kids to share their profiles and blogs with you.

SAFETY TIPS FOR CYBERBULLING

Cyberbullying: The use of information communications technology (particularly mobile phones and the Internet) to deliberately offend someone else.

Using the Internet and technology should be a positive experience for young people. Unfortunately, technology can be used in negative ways. When a young person is bullied or harassed via the Internet or cell phone by their peers, the Internet is no longer a safe or enjoyable place and instead becomes a source of anxiety and fear. In various research studies conducted around the world, as many as **one-third of young people surveyed have experienced cyberbullying**. Young people can be participants as much as they can be victims of cyberbullying, and there are risks to anyone who engages in such behavior. Harassing or bullying anyone online can even be considered a criminal offense.

How is technology used to bully? Below is a list of both positive and negative ways that technology can be used:

Technology	Great for…	Examples of misuse
Mobile Phones	Keeping in touch by voice or text, taking and sending pictures and film. Useful in emergency situations and for allowing children a greater sense of independence.	Sending nasty calls or text messages, including threats, intimidation, and harassment. Taking and sharing humiliating images. Filming others being harassed and sending them to other phones or Internet sites.
Instant Messenger (IM)	Text or voice chatting live with friends online. A quick and effective way of keeping in touch.	Sending nasty messages or content. Using someone else's account to forward rude or mean messages via their contacts list.
Chat rooms and message boards	Groups of people around the world can text or voice chat live about common interest. This can be an easy way to meet new people and explore	Sending nasty or threatening anonymous messages. Groups of people deciding to pick on or ignore individuals. Making friends under false pretenses – people pretending to be someone they're not in order to gain personal information that can be misused in a

	issues which they are too shy to talk about in person.	range of ways – e.g. by spreading secrets, blackmailing, or luring.
Email	Sending electronic letters, pictures, and other files quickly and cheaply anywhere in the world.	Sending nasty or threatening messages. Forwarding unsuitable content including images and video clips, or sending computer viruses.
Social networking sites	Socializing with your friends and making new ones within online communities. Allowing young people to be creative online. Personalizing profiles and homepages, creating and uploading content.	Posting nasty comments, humiliating images or videos. Accessing another person's account details and sending disturbing messages, deleting information or making private information public. Groups of people picking on individuals by excluding them. Creating fake profiles posing as someone else.

Below are some safety tips that parents, teachers, and caregivers can give to young people on the topic of cyberbullying:

1. Only post online what you would comfortably share with your entire class.
2. Be nice online.
3. Do not retaliate.
4. Report bad behaviour to someone you know.
5. Report bad behaviour to the service provider.
6. Save the evidence.
7. Choose not to participate.

HOW TO RECOGNIZE ONLINE GROOMING

Sometimes the very reason kids and teens blog and spend time on social-networking sites is to "meet new friends." So it is not always easy for them to tell when "new friends" have bad intentions, and research has shown that as many as **14% of kids receive unwanted sexual solicitations online**.

"Grooming" is a method used by sexual predators to sexually exploit children. Grooming is manipulation. The goal of this kind of pedophile is to **target** young people online and to eventually meet them offline. It can involve flattery, sympathy, offers of gifts, money, or modeling jobs. Most of these techniques are employed over extended periods of time, hence the term "grooming." Experts say the short-term goal of these manipulators is for the victim to feel loved or comfortable enough to want to meet them in person, which takes time. Groomers tend to have a lot of patience. They also "work" a number of targets at once, telling all of them that they are "the only one for me." You can imagine how effective this can be for a child seeking sympathy, support, or validation online. This is a very general explanation because grooming is **carefully individualized**. Groomers design what they say as they go along, tailoring their flattery or offers as they learn about the victim.

Here are some tactics to watch out for:

Tactic	**Intent**
"Let's go private."	Engage in private conversation through a separate chat room, instant messaging, or phone texting
"Where's your computer in the house?"	Determine if parents or caregivers are in close proximity
"Who's your favourite band? Designer? Film? Gear?"	Discover what types of gifts to offer - e.g. concert tickets, clothing, CDs

"I know someone who can get you a modeling job."	Flattery
"I know a way you can earn money fast."	Appeal to a young person's natural interest in earning spending money
"You seem sad. Tell me what's bothering you."	Show sympathy to encourage child to confide in groomer and potentially pull them away from family support
"What's your phone number?"	Establish off-line contact - usually happens at a later stage, after the target feels comfortable with the groomer
"If you don't... [Do what I ask], I'll... [Tell your parents OR share your photos in a photo blog / Webcam directory / file-sharing network]."	Intimidation and manipulation – used as the groomer learns more and more about the target
"You are the love of my life."	Manipulation - becoming appealing to someone by making him or her feel special and building companionship

Parents and caregivers should speak with their kids about these tactics, and kids should know to inform their parents or caregivers or teacher if they ever encounter them.

Being aware of the signs of online grooming and the fact that groomers are self-taught experts in 1) getting kids to reveal their needs and desires and 2) tailoring messages to those interests can go a long way toward protecting kids from sexual exploitation online. It's also a great exercise in critical thinking, the best safeguard and "filter" a young Internet user can have.

If you believe your child or a child you know may be a victim of grooming, please contact the organizations below:

- **Canada: Cybertip.ca - www.cybertip.ca**
- **US: National Center for Missing and Exploited Children - www.CyberTipLine.com**