LEARNER INTERNET SAFETY GUIDELINES

CREATING PASSWORDS

Passwords are used to access personal information stored on a Web site or on your computer. Although your password should be easy for you to remember, you will need to change it often. Why? Because passwords obtained by fraudsters or thieves can be used to gain access to your financial accounts or private information, or to impersonate you when applying for credit, opening bank accounts or purchasing products.

Protecting your passwords

- Create passwords with a combination of at least eight letters and numbers, and use both upper- and lower-case letters. Longer passwords are harder to decipher. Think of a phrase or sentence meaningful to you and easy to remember
- Then, take the first character from each word, alternate upper and lower case and use some common letter-number substitutions
- Avoid the use of personal information as part of your password
- Do not use your name, your pet or child's name, your Social Security number, or your current or former address
- Stay away from number or letter patterns and sequences (for example,"121212" or "abcdefg")
- Change your password every 60 to 90 days
- Vary your password — do not use the same one for every account or retail site
- Use a password that differs from your screen name
- Do not store your password online

SAFEGUARDING YOUR PRIVACY

You can never be sure who you are chatting with online. The friendly fellow movie fan or book lover in an online forum may actually be a clever criminal looking for his next cybercrime victim. How can you have fun online while protecting yourself?

Do not post information that will identify you, including:

- Your full name
- Your home address or phone number
- Passwords
- Credit card or bank account numbers
- Names of family members or friends
- Your workplace or favourite hangout
- Names of clubs or organisations to which you belong
- Historical information that could identify your past residences
- Do not use a nickname that can be used to identify you
- Never share your account password

STAYING SAFE USING BLOGS, CHAT ROOMS, E-MAIL, INSTANT MESSAGING

Fast friendships are forged over the Internet — and there is no doubt that casual, online conversations sometimes are the foundation of good, lasting relationships. However, the anonymity of the Internet may compel some individuals to reveal too much about their private lives or to make hurtful comments or accusations they would never make in person. If an online conversation makes you uncomfortable in any way, sign off immediately. It is important to remember that the rules of behaviour that apply in "real life" apply to your "cyber life," too. Think about how your e-mail message will be read by others. Do not say anything online that is cruel or may damage someone's reputation. Doing so puts you at risk of being accused of slander or defamation, or may cause a dangerous escalation of hostilities.

- Do not give out personal information about someone else
- Do not forward another individual's e-mail without their permission
- Never allow anyone to photograph you in an embarrassing or compromising situation
- Never post anything that would cause you embarrassment or shame

The **Internet** is the most public of forums — once you have posted a comment, a photo or a video, it cannot be erased or taken back. You cannot control its duplication and it may be used against you. Do not send photos of yourself or family members to Internet acquaintances. Photos can be altered and sent to others, and elements in photos— a landmark or a street name, for example — can be used to identify your location.

Remember that, once posted, the information can be seen by anyone with a computer and an Internet connection: family and friends, employers or potential employers - even police and other law-enforcement authorities.

INTERNET BULLYING

Known as cyberbullying, it occurs in all communities and at all income levels. Sometimes, the bully is someone you know. But the bully may be an individual you have never met —perhaps someone angered in a chat room or on a gaming website. Cyberbullying can be more harmful and frightening than schoolyard bullying, because it is very public. The bully spreads hurtful comments or innuendos to many individuals via the Internet, and others may join in.

If you suspect you or your child is the victim of a cyberbully:

- Use the block feature to block the sender's e-mail or instant messaging (IM) account
- Warn the bully that if the behaviour does not stop, you will inform the Internet Service Provider (ISP) and the appropriate authorities
- Save every communication from the bully
- Report the situation to the ISP
- Stay offline, if necessary

PROTECTING YOUR CHILDREN WHILE THEY ARE ONLINE

As a parent, it is your responsibility to know what your children are doing online and guard them against the dangers that prey on unsuspecting minors. How can you do that?

- **Set parameters:** How many hours a day can they spend online? What sites can they visit? Are chat rooms OK or off-limits? What about interactive games? Set rules and enforce them.
- **Keep the family computer (or your child's computer) in a busy area :** Children, especially young children, should access the Internet where you can monitor them and monitor the sites they visit. Consider installing a software program that allows you to control their Web browsing. If your children have e-mail accounts, make sure you know their passwords and randomly check messages.
- **Educate yourself and your children:** Follow news reports and conduct research to find real-life examples of Internet predators. Remind your children that individuals they "meet" online are not always who or what they seem
- **Encourage your children to talk to you:** Ask them to alert you if they encounter someone or something online that makes them uncomfortable. Remind them that you will not be angry; you love them and want to protect them from real danger.
- **Look for signs that your child might have been targeted by an online predator:** If your child is secretive, unusually quiet or spending too much time online, ask questions and be supportive.

Signs that your child might have been targeted by an online predator:

- Uncharacteristic silence or withdrawal from the family
- Turning off the monitor or reducing a Web page when you enter the room. If this is happening, log on to your child's computer and look for evidence of inappropriate sites. Ask for expert help, if necessary. "Google" your child's name to see if his personal information is on the Internet
- Spending a lot of time online — especially at night, when most computer predators are online, too
- Making or receiving telephone calls to or from unrecognised numbers