LONDON'S GOOD INTERNET SECURITY PRACTICES

1. Protect your computer by using a firewall, anti-virus software and other security measures. An increasingly common practice is the use of malicious code (viruses, worms and Trojan horses) to acquire the personal information needed to commit identity theft. Consider the use of an anti-phishing toolbar or anti-phishing enabled web browser such as Internet Explorer or Firefox.

2. Ensure your browser is up to date and that security patches have been applied. For example, Microsoft Internet Explorer browser users should immediately go to the Microsoft Security home page - http://www.microsoft.com/security/ - to download a special patch relating to certain phishing schemes.

3. Be suspicious of e-mails from financial institutions, Internet service providers and other organizations asking you to provide personal information online. Reputable firms never ask for personal information in this manner. If you are at all uncertain, look up their phone number in the phone directory, or use the number printed on the back of the credit card or account statement, and call. Clues to fraudulent e-mails include a lack of personal greetings and spelling or grammatical errors.

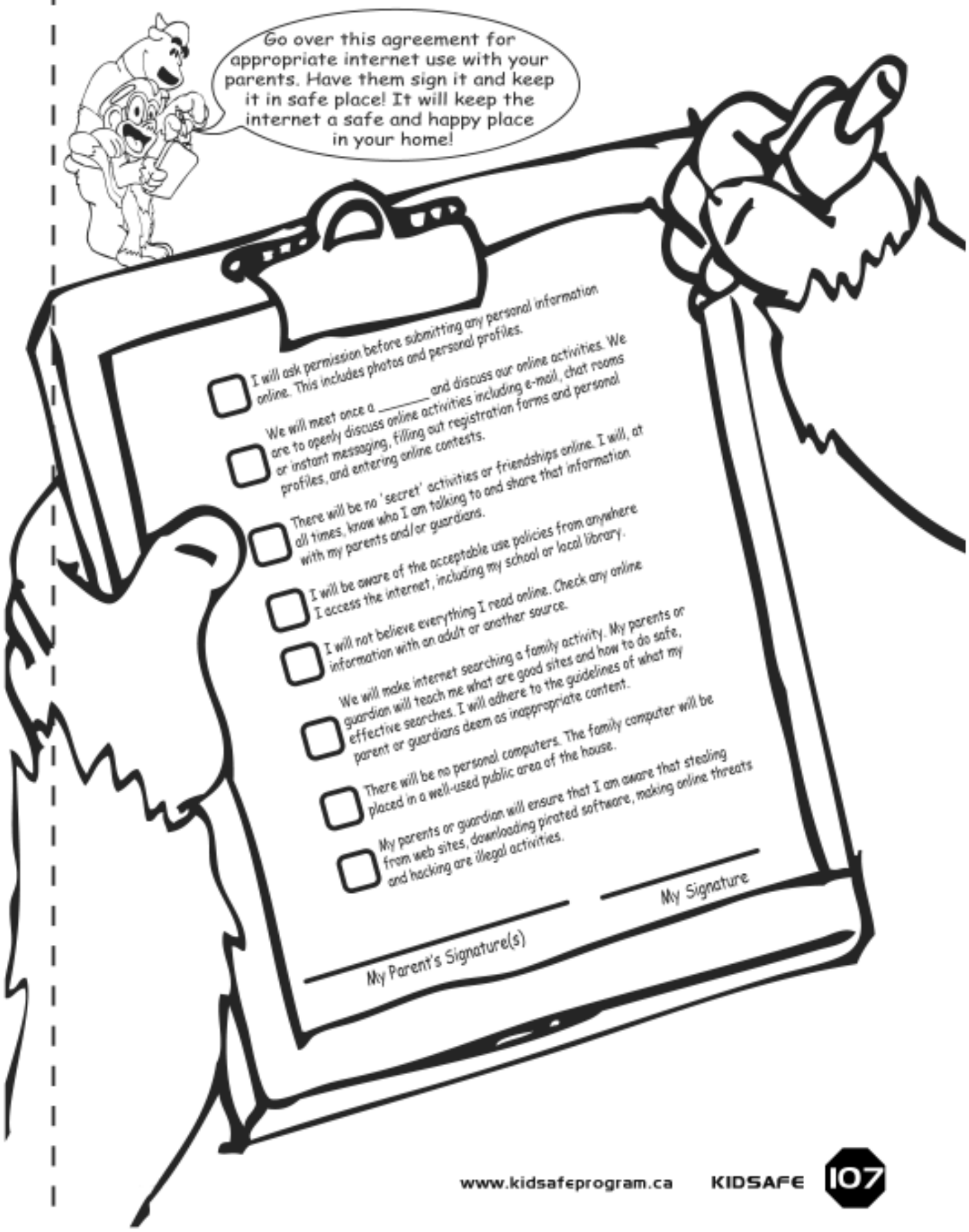
4. Always ensure you are using an authentic, secure web site when submitting credit card or other sensitive information. Start by typing the web address into the browser address bar manually. Once you are at the site, make sure you're on a secure web server by checking the beginning of the web address in your browser's address bar - it should be "https://" rather than just "http://". There should also be a small yellow padlock symbol in the lower-right hand portion of your screen.

1. To avoid Internet “phishing” sites, never click on links in the e-mail or cut and paste them into your browser - chances are the link will take you to a fake web site. It is safer to log onto the web site directly by typing the web address in your browser.

2. Never call a telephone number provided in a phone call or an e-mail regarding possible security issues with a credit card or bank account. Only the phone number on the back of a credit card or bank statement is a valid number to discuss credit card account information.

3. If any suspicious or unfamiliar "buttons" or other "clickable" items appear on a web site that you frequent, such as a MySpace page, do not click on them until you have verified their authenticity. If you accidentally click one of these items do NOT provide any information that you may subsequently be prompted for. Spear phishers may have embedded malicious code directly in personal web pages.

4. If, for any reason, you believe or suspect your personal information may have been compromised, contact the relevant institutions (i.e., your bank, credit card issuer, credit reporting bureaus, or utility provider) as soon as possible. If you believe a crime has been committed or attempted, you should also contact local law enforcement. You can also report any suspicious activity to one of the online organizations, listed in the next section, after contacting these authorities.


Go over this agreement for appropriate internet use with your parents. Have them sign it and keep it in safe place! It will keep the internet a safe and happy place in your home!
I will ask permission before submitting any personal information online. This includes photos and personal profiles.
We will meet once a _____ and discuss our online activities. We are to openly discuss online activities including e-mail, chat rooms or instant messaging, filling out registration forms and personal profiles, and entering online contests.
There will be no 'secret' activities or friendships online. I will, at all times, know who I am talking to and share that information with my parents and/or guardians.
I will be aware of the acceptable use policies from anywhere I access the internet, including my school or local library.
I will not believe everything I read online. Check any online information with an adult or another source.
We will make internet searching a family activity. My parents or guardian will teach me what are good sites and how to do safe, effective searches. I will adhere to the guidelines of what my parent or guardians deem as inappropriate content.
There will be no personal computers. The family computer will be placed in a well-used public area of the house.
My parents or guardian will ensure that I am aware that stealing from web sites, downloading pirated software, making online threats and hacking are illegal activities.
My Parent's Signature(s)
My Signature