

How can I get more information about securing my computer?

Here are a list of sites that provide more detailed information about securing your home computer from outside threats.

http://www.cert.org/tech_tips/home_networks.html

<http://www.staysafeonline.org/>

http://www.cheycobb.com/home_security.html

<http://iserloh.com/oped/safecomputing>

<http://security.uwo.ca/homecomputer.html>

<http://www.markusjansson.net/eseuring.html>



LABRADOR
DISTRICT SCHOOL BOARD

Data Security Best Practices



LABRADOR SCHOOL BOARD
www.lsb.ca

What should I transport the data home?

If you need to work on personal and/or confidential data on a computer outside of school then please use the following method.

Encrypted USB/Flash Drive if you do not currently have a flash drive that supports file encryption, please contact the Information Technology Department about upgrading your existing Flash Drive or obtaining a new one.

What else can I do to protect the data during transporting?

Try to limit the amount of personal information being taken home. (For example take just the student name and not other student identifying information)

Use Password protected files. For example, Microsoft office and Corel documents can be password protected. For information on how to password protect documents please contact the Information Technology Department.

Zip files using WinZip 11 and password protect the files before transporting them. For information on how to use WinZip 11 please contact the Information Technology Department.

Don't use email as a method to transmit confidential or personal information across public networks such as the Internet unless the email and/or attachments are encrypted or zipped in a secure manner.

Use of CDs and DVDs to transport confidential or personal information is not recommended. While there may be situations where these methods must be used for backups (e.g. where there is no access to a network for backups), in such situations, you should make two copies for storage in two separate secure physical locations. The files in the CDs/DVD containing confidential and/or personal information should be carefully managed.

Wireless networks should not be considered entirely safe even with security enabled. You should not connect any device containing personal and/or confidential information to a wireless network.

How can I protect the data while editing it on a non-school computer?

To ensure that the data is safe on the non school computer while you work on it, the following computing practices are recommended.

Disconnect Computer from Network

If possible, please remove the computer from all networks that are exposed to the internet before working on the data.

Disable File Sharing Programs

Please disable all file sharing programs (e.g. LimeWire, Bearshare, Utorrent) since these programs open ports which could be used to access your computer.

Disable Chat Programs

Similar to file sharing programs, Chat programs (e.g. MSN Messenger, ICQ) open ports, which could be used to access your computer.

Remove Files when Finished

Once you have finished working on the file and saved it to an encrypted USB/Flash drive then remove it from the computer before you connect your computer to the internet. Remember to empty the recycle bin after you delete the file(s).

Delete Temporary Internet files

Most spyware programs hide in the temporary files that are left on your computer after you use the internet. To remove these files please use the menu option available in Internet Explorer and Firefox.

Run Spyware if anti-Spyware has not been run on that day then run your spyware program before editing your files.

Run Virus Checker if virus checker has not been run on that day then run it before you edit a confidential file.

Read your Computer Manuals

New electronic devices have more features, which mean that you will have more of a "learning curve" to be able to understand and use these items properly. Default settings are often the least secure for devices, and if left that way everyone who has the same device will have the same default settings.

Harden your system

Find and use techniques to tighten the security of your system. Base installations of Operating systems often have standard defaults that leave the system vulnerable. Here are a few helpful websites:

<http://www.firewallguide.com/tighten.htm>

<http://www.lbi.gov/ITSD/Security/systems/wxp-security-checklist.html>

***Note: Update Spyware and Virus Checker weekly and ensure they are not expired.**