Cyber Security Guidelines
WCSB Teachers
Teacher's Guide to Computer Network Security

These guidelines are intended to help you to be an informed and responsible professional.

1. **Passwords should be well protected.**

   Passwords should never be shared or given to anyone. They should not be written down and stored in a place where others can see or find them.

2. **Secure your desktop and mobile devices**

   Computers should require a log-in password and should be locked automatically after a period of inactivity. Always log out/sign off when you are finished with your computer. It's quick, easy, and may save your account from unwanted trespassers. Remember, you are responsible for all school board devices that are assigned to you.

   If you are using a public terminal, exit the browser you are using when you are ready to end your Internet session. Be sure to clear your history and your cookies

3. **Create regular back-ups of self-created documents**

   It is your responsibility to save your self-created school related documents on a storage device (server, thumb-drive, CD, etc.)

4. **Use safe email and download practices**

   a. Never download or open an attachment or reply to an email you were not expecting or which looks suspicious, even from someone known to you. (E-mail addresses can be spoofed.)
   b. Do not reply to spam e-mail messages or other harassing or offensive email. By responding, you only confirm that you are an actual person who can be spammed.
   c. Always use caution when revealing personal information, such as your social security, birth date and home address, to anyone you communicate with through email. This is true even if the person purports to be someone of authority.

5. **Be sure your anti-virus software is installed and up-to-date at all times**

   Confirm that the computer's virus protection program is working properly. Be sure anti-virus software is configured to scan all devices that are attached to the computer.

6. **Treat student data with extreme privacy**

   Protecting the privacy of students is a professional responsibility. Be very careful about personally identifiable confidential data on your computer, back-up disc, laptop, mobile PDA or posted on the internet. *(Do not send attachments or text with student-related information through email.)*

7. **Take special care of your personal information**

   Never give out your Social Security Number or other personal information online at websites, in chat rooms, or in email. Be aware that emails sent from your school board email address are public record and should only be used for school business

8. **Monitor all online activity of your students**

   As a teacher; you are responsible for being vigilant and monitoring student computer use. Report any suspicious incidents to your site administrator as soon as you become aware of them. Do not turn off the computer unless instructed to do so by your site administrator.