Annapolis Valley
Regional Centre for Education

Privacy Checkup

As an employee of a public body, you have a responsibility to keep personal and sensitive information secure. This privacy checkup will help you identify areas where you may need to improve privacy measures. A 'no' answer to any of these questions is a warning sign that information may not be secure.

Physical Security

Do you have files with sensitive information stored in your office/classroom?

- If yes, is this information stored in a locked filing cabinet?
- Do you lock your office door whenever you leave?

At the end of the day do you:

- clear your desk of all files with sensitive information?
- store your laptop and files in a locked filing cabinet?
- lock your office/classroom door?
- log off your computer?
- remove documents with sensitive information from faxes and printers?

Email & Faxing

Before **emailing** sensitive information do you:

- ensure that the owner of the sensitive information has consented to sending via email?

Before **faxing** sensitive information do you:

- call the receiver to confirm that the receiving fax machine is secure and confirm the fax number?
- use a cover sheet that includes both both the sender and recipent information?
- attach a confidentiality notice?

Security of Electronic Files

- Do you login to any system using a unique identifier and password?
- Is your password complex (numbers, symbols, letters, etc.)?
- Have you changed your password in the last 90 days?
- Do you store electronic files containing sensitive information on a secure central server? (no sensitive information stored on local hard drive)
- Is your computer screen positioned so that no unauthorized individuals can view sensitive information displayed?
- Is your screen saver set to automatically log out after a 5 minute period of inactivity?

Mobile & Portable Devices

- Do you store mobile or portable storage devices such as laptops in a locked cabinet when not in use?
- Is sensitive information saved on portable storage devices limited to the absolute minimum necessary?
- Do you permanently delete sensitive information as soon as possible after use?

Privacy Habits

- Do you avoid discussing personal information in areas (including social media) where conversations can be overheard by unauthorized personnel?
- Do you disclose personal information to co-workers only where the information is necessary for them to do their work?
- If you must travel with personal information, do you ensure that it is stored in a locked cabinet and never in your car?

Secure Disposal of Sensitive Information

- Do you dispose of hard copy records containing sensitive information by placing them in a secure shredding bin or by shredding them yourself?

~ adapted from Office of the Information and Privacy Commissioner for Nova Scotia, 5 Minute Privacy Checkup