# Security of Electronic Media and Personal Information

**PIM Toolkit, 9-13;**

**What practical tips can I offer staff about PIM, particularly electronic media?**

Here are some suggestions that will allow them and you to feel more assured that privacy and confidentiality will be maintained:

- **Flash drives, USB keys, etc.** – Use only if encryption is built into the hardware. Issue one that meets board standards to staff. Know where it is at all times. Consider wearing it on a lanyard, around your neck. "Process" (erase) the drive, to ensure all personal information has been eliminated, if another employee will use it.
- **External Back-up Storage –** For sensitive material, avoid using servers outside the country.
- **Report Card Writing –** If possible use web-based systems. Log in with a secure password and remember to log out. In fact, log out of all applications or a browser. Work in a location where others' views of the screen are minimized. Adopt a "clean desk" model whereby you limit the amount of sensitive, personal or confidential data in that area. Take all notes, student portfolios and other records with you at the end of your work session.
- **Working with Your Students' Confidential Information at Home –** Exhibit care for records when traveling to and from school. Discreetly label folders or envelopes. Limit the amount of confidential information you bring home. Work in an area that is designated as "secure". At home, avoid storing student information on a shared network drive. If you have an answering machine, use one with multiple mailbox capabilities so callers can direct sensitive information to you. Ensure that access to your voice mailbox is password-protected. Avoid discussing students at your dinner table. Monitor who has access to your home's fax machine and printer, particularly if the printer is networked.
- A secondary school office has many more individuals (office manager, secretaries, attendance personnel, volunteers, etc.). Instruct all personnel in the procedures and protocols of privacy. Highlight not only the day to day management and protection of information and privacy, but the verbal discussion of student situations, with each other and with students and other visitors.

**Principal's Best Practice:** Conduct a "self-audit" using the PIM Toolkit's "Privacy Awareness Checklist". Every staff member, including the principal, could do this in September. Then reassess at the end of the school year. The following year, go over this with new staff. You could also have volunteer PIM champions in this area i.e. staff members that would be willing to assist their colleagues.