

## Electronic Information

**What guidelines are there with respect to managing electronic information?** PIM Toolkit, 9, 10

As principal, you face the challenge of staff using electronic equipment to manage information. Benefits occur with ease of use, speed and storage capabilities, but these are usually offset by compounded responsibility to ensure that privacy and confidentiality are maintained. MFIPPA, PHIPPA and PIPEDA outline security responsibilities. The school principal ought to consider the following:

Effective management of passwords for all technology and software applications, including: desktop and laptop computers, smart devices such as BlackBerry's, PDA's, iPhones, etc. Passwords are a security measure for the protection of personal and confidential information. Additionally they protect your identity because a person that has your password can be you in the online world. Check with your board's IT department with respect to password protocols. Storage of personal data should be on encrypted devices and storage platforms i.e. flash drives, USB devices, board servers, etc., and not shared network drives. Never store student personal information on a home computer. Secondary school principals and staff need to be especially vigilant. Tests and other documentation may be more apt to be stored and exposed inadvertently.

Protect access to email.

Computing should be done in private areas where possible. Screens should be positioned to minimize viewing of information. Monitors should be locked when unattended or not in use (windows key + L).

Also, ensure that all copies sent to printers, fax machines, etc., are retrieved immediately. If I notice confidential information has been left lying about, do I bring it to the owner?

Before sending personal, confidential, or sensitive information via email, have I considered taking precautions such as removing or limiting personal information? Have I confirmed address fields?

Documents containing personal or confidential information should be disposed of by shredding.

Electronic records containing personal or confidential information should be disposed of by secure destruction. MFIPPA regulations require personal information to be retained for 12 months after the last time it was used *at a minimum* unless the individual to whom the information relates agrees with you to destroy/delete it sooner.

**Principal's Best Practice:** Cover this information at a staff meeting. Invite staff to bring all mobile computing and storage devices they own. Divide the group into teams and have them devise

scenarios where private or confidential data is comprised because of lax use of these devices. Brainstorm around safe practices for all these devices. Compare the group's ideas with guidelines that have been developed by your board or the OIPCO.

**What needs to be considered when a school or board is transitioning from paper to electronic records?** [PIM Toolkit, 44](#)

Precedents are still being set in this area. For example, the Ministry of Education has given school boards permission to move from hard copy attendance records/systems to electronic when a board feels it has satisfied the requirements for doing so. Report cards are done using electronic and online formats but OSR Guidelines require an exact hard copy to be filed.

To determine whether or not paper is required, several actions must be taken:

- Establish electronic records policies and procedures, based on the Canadian General Standards Board standard "Electronic Records as Documentary Evidence."
- Prioritize records to convert, or maintain electronically.
- Identify the legislation and/or guidelines which govern the creation and management of the records.
- Determine whether or not there is a requirement to maintain a paper copy, and why.
- Discuss the risk of not maintaining a paper copy with business owners, Records and Information Managers, Legal, and Information Technology staff.

**Is it permissible to switch any paper record to its corresponding electronic version?**

Although it may seem like a good idea, you should check with your board's PIM Champion, Records Manager or MFIPPA Officer. There may be situations where hard copies are required, such as in the case of evidence required at a trial or where hard copy signatures are required.

**Principal's Best Practice:** Consult with your Superintendent of Education and determine if your plans for converting documents is in line with district plans and what other principals in your board are doing.