PURPOSE

The use of mobile technologies in the course of daily work is becoming very common for school board/authority employees. Mobile devices can enhance the quality of work and life for employees, but they also dramatically increase the risk for data loss and personal information disclosure. The following guideline is intended to assist school boards/authorities in identifying areas of risk involving mobile devices and provide strategies for the development of an internal procedure or regulation.

Overview

When working both at the office or school and offsite, school board/authority employees must comply with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). The Act requires that organizations protect the privacy of individuals with respect to personal information about the individual held by the organization. This Act can be found at the Information and Privacy Commissioner's website: http://www.ipc.on.ca.

This guideline reflects best practices for securing mobile devices owned by a school board/authority, including but not limited to laptop computers, jump drives, cell phones, and PDAs, along with the personal information stored on these devices. The first principle of privacy is accountability. When personal information is in the care and/or custody of school board/authority employees, they are personally responsible for ensuring that privacy is protected.

Data owned by a school board/authority is not to be maintained or stored on any personally owned mobile devices. The major recommendations are:

- Personal information, to the greatest extent possible, should not be stored on mobile devices.
- Personal information, if stored on mobile devices owned by a school board/authority, should be:
  - Password-protected and/or securely encrypted.
  - A copy only-not the sole instance of the data.
- Personal information should always be transmitted in a securely encrypted format and never by email.
- Portable devices and storage media with personal information should be destroyed or erased so that there is no possibility of subsequent data recovery.

General Guidelines

Due to the inherent risks involving mobile devices, these should always be considered insecure and therefore require protection according to the following guidelines.

1. **Electronic Records/Mobile Device:** To the greatest extent possible, personal information should not be stored on or accessed from mobile devices. This simple rule does much to reduce risk.
2. **Data Encryption:** If personal information must reside on a mobile device, it should be encrypted. The decryption key should be entered manually; this step should not be automated. A means should exist to recover encrypted data when the decryption key is lost. Whole-disk encryption is potentially the most secure option

available. Since encryption standards are always evolving, school boards/authorities are responsible for ensuring that any solution selected meets the generally accepted standards in effect at the time. Encryption installations need to be regularly reviewed and updated as necessary. If in doubt, please refer to your Information Technology Team for support.

3. **Multiple Copies of Data:** Personal information residing on mobile devices should not be the only copy. Make sure there is another copy on a more secure device such as a server that is backed up regularly.

4. **Data Destruction:** The normal process for deleting data from a hard drive, USB flash drive, cell phone memory, etc., does not completely delete the data. Tools are readily available to easily recover deleted data and even fragments of files from these devices. Even if data is encrypted, it has to be decrypted for use and may therefore exist unknowingly in decrypted form in a temporary file that can be recovered even after deletion. Consequently, sensitive data should be destroyed or erased so there is no possibility of subsequent data recovery. Mobile devices and other electronic equipment that contain or access personal or confidential information, or have been used to access sensitive information in the past, should be processed to ensure all data is permanently removed in a manner that prevents recovery before these devices are redistributed to another employee, disposed of as surplus equipment, or returned to the vendor.

5. **Password Protection:** Access to the mobile device should be protected by the use of a strong password. Please refer to the PIM taskforce password guideline for strong password. On mobile devices, do not automate the supplying of passwords or other security credentials needed to access sensitive data (for example, automatically authenticating to an application or database that contains sensitive information, or having Microsoft Windows store passwords to these systems).

6. **Password Storage:** User IDs and passwords permitting access to the mobile device should never be stored in "plain text" (i.e., unencrypted so they can be easily read) on mobile devices.

7. **Physical Protection:** Reasonable care should be taken when using mobile devices in public places, meeting rooms, or other unprotected areas to avoid unauthorized access to or disclosure of the information stored on or accessed by the device.

   Special care should be taken in crowds, meetings, and security-screening areas to maintain control over the device. Do not let it out of your sight.

   - Mobile devices should not be left unattended and, where possible, should be physically locked away or secured. Use a cable lock with an audible alarm when not working on them,
   - Mobile devices should be transported as carry-on luggage whenever travelling by commercial carrier unless the carrier requires otherwise.
   - Do not leave mobile devices containing personal information in your vehicle. (If it absolutely cannot be avoided, lock them in your trunk before you start the trip, not in the parking lot of your destination or in other places where you can be publicly observed. If the vehicle does not have a trunk, leaving the device in the vehicle is not a secure option.)
   - All mobile devices should be discreetly and permanently marked as school board/authority property and should indicate a method of return in case the device is lost.
   - Enable the automatic lock feature of your device after five minutes or more of idle time.

- Conduct confidential work only on mobile devices over which you have control. Do not use public computers or networks or work on personal or confidential material in public places, and do not perform this type of work on computers that are shared with family members.
- While viewing personal information on a mobile device screen at locations outside the office, ensure that the screen cannot be seen by anyone else. Personal information should never be viewed on a mobile device screen while in the public.
- Software tracking and protection should be employed wherever possible. This may take the form of an inventory system to track the devices and/or a centrally administered software solution that can force passwords and security policies for mobile devices.

8. **Virus Protection:** Any mobile device capable of using antivirus software and anti-spyware programs should have the software installed and configured to provide real-time protection. The programs must be updated regularly with the latest security patches.

9. **Cell Telephones:** When in transit or working outside the office, employees should avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard or intercepted by individuals using scanners or other devices.

10. **Training Related to Mobile Devices:** Employees should be trained on the proper usage of the mobile device. Training should include privacy and security requirements as well as responsibilities for appropriate care of information according to these general guidelines.

11. **Loss or Theft of Mobile Device:** A privacy breach occurs when personal information is collected, retained, used, or disclosed in ways that are not in accordance with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*. Among the most common breaches of personal privacy is the unauthorized disclosure of personal information, contrary to section 32 of the Act. For example, personal information may be lost, stolen (especially from laptop computers, a prime example), or inadvertently disclosed through human error, and upon learning of a privacy breach, immediate action should be taken. Users should contact their FOI Coordinator immediately or refer to their Board's Privacy Breach Procedure.

References

Kansas State University, Information and Privacy Commissioner Office