Section: Business and Administrative Services
- Administrative Operation

Regulation Code: BA-1.8.2
Policy Code Reference: BA-1.8
Regulation: SECURING MOBILE DEVICES

This administrative regulation is written in accordance with the guiding principles in Board Policy No. BA-1.8, Privacy and Information Management.

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. When working both at the office or school and offsite, school board employees must comply with the Municipal Freedom of Information and Protection of Privacy Act. The Act requires that organizations protect the privacy of individuals with respect to personal information about the individual held by the organization.

The purpose of the Securing Mobile Devices administrative regulation is to ensure that all board-owned and personal mobile devices and the sensitive information stored on or accessed from these devices is protected at all times. Mobile devices can be considered to be any portable technology used to store or access information. They include but are not limited to:

- laptop computers, tablets
- jump drives, USB keys, Bluetooth storage keys
- external hard drives or other storage devices
- Smartphones

1. General Rules – Use of Mobile Devices

The following general rules apply to using mobile devices:

1.1 Sensitive information, to the greatest extent possible, should not be stored on or accessed from Smartphones, USB devices, external hard drives or personal laptops. This will do much to reduce risk.

1.2 Sensitive information, if it must be stored on or accessed from mobile devices, should be:

1.2.1 password protected and/or securely encrypted.

1.2.2 a copy only, not the sole instance of the data. Another copy must reside on a board-provided home drive or a board server that is backed up regularly.

1.3 Sensitive information should always be transmitted in a securely encrypted format and never in clear-text by email.

1.4 The normal process for deleting data from Smartphones, USB devices, external hard drives, personal laptops, etc., does not completely delete the

data. Tools are readily available to easily recover deleted data, and even fragments of files, from these devices.

Board-owned portable devices and storage media with sensitive information should be returned to the Information and Communications Technology (ICT) Department to be destroyed or erased when no longer needed so there is no possibility of subsequent data recovery.

2. Password Protection

2.1 Password Use

Access to the mobile device should be protected by the use of a strong password. Please refer to Administrative Regulation No. BA-1.4.5, Technology Standards Password Management. Passwords should never be automatically saved on mobile devices.

2.2 Password Storage

When accessing websites or applications, never save your password in "plain text" (i.e., unencrypted so the characters can be easily read).

3. Physical Protection

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

3.1 Mobile devices should not be left unattended and, where possible, should be physically locked away or secured. A cable lock should be used on laptops when not in use or they should be secured in a locked cabinet.

3.2 Mobile devices should be transported as carry-on luggage whenever travelling by commercial carrier unless the carrier requires otherwise.

3.3 Mobile devices containing personal information must never be left in vehicles. If it absolutely cannot be avoided, the device should be locked in the trunk before leaving for the destination, not in the parking lot on arrival.

3.4 All mobile devices should be discreetly and permanently marked as school board property and there should be a method of return indicated in case the device is lost.

3.5 The automatic lock feature of the device should be activated after ten minutes or less of idle time.

3.6 Public or loaned laptops should never be used for confidential work and confidential material should not be worked on in public places.

3.7 While viewing personal information on a mobile device screen at locations inside or outside the office, the screen should not be visible to anyone else.

3.8 All mobile devices capable of using antivirus software and anti-spyware programs should have the software installed and configured to provide real-time protection. The programs should be updated regularly with the latest security patches.

3.9 When in transit or working outside the office, cell phones should not be used to discuss sensitive or personal information. Cell phone conversations can be easily overheard or intercepted by individuals using scanners or other devices.

3.10 Mobile devices shall always be running support operating systems and have all required security patches applied.

4. Training Related to Mobile Devices

Employees must ensure that they receive training on the proper usage of the mobile device. Training should include privacy and security requirements, as well as responsibilities for appropriate care of information per this administrative regulation.

5. Loss or Theft of Mobile Device

Personal information may be lost, stolen (laptop computers are a prime example) or inadvertently disclosed through human error. Any of these circumstances constitutes a privacy breach under the Municipal Freedom of Information and Protection of Privacy Act. Upon learning of a privacy breach, immediate action must be taken. The employee must contact their supervisor and the Freedom of Information (FOI) co-ordinator immediately.