

KAWARTHA PINE RIDGE DISTRICT SCHOOL BOARD

ADMINISTRATIVE REGULATIONS

---

Section	Business and Administrative Services	Regulation Code: BA1.8.2
	• Administrative Operation	Policy Code Reference: BA1.8
Regulation:	SECURING MOBILE DEVICES	Page 1

---

This administrative regulation is written in accordance with the guiding principles in Board Policy No. BA1.8, Privacy and Information Management.

## KAWARTHA PINE RIDGE DISTRICT SCHOOL BOARD

Section: Business and Administrative Services

Regulation Code: B-1.8.2

• Administrative Operation

Policy Code Reference: B-1.8

Regulation: SECURING MOBILE DEVICES – continued

Page 2

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.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.

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.

