MOBILE DEVICE SECURITY

Background:

The Division supports the use of mobile devices to facilitate educational and business activities and provide access to the internet and Division resources. The Division recognizes the importance of balancing risk with responsible use.

Definitions:

Division Network:
includes all wired and wireless computer networks in the Division.

Information Technology Asset (IT Asset):
includes all Division-owned equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. This includes assets such as servers, computers, laptops, mobile devices, tablets, wireless networks, printers, copiers, fax machines, scanners, displays, projectors, audio systems, monitors, firewalls, routers, switches, memory devices and software. Although peripherals and consumables—for example keyboards, mice, web cameras and chargers—form part of the asset, they're not subject to asset control.

Mobile Devices:
includes Division-owned and personally owned portable technology—laptops, mobile phones and tablets.

Security:
is the continual analysis and management of risks.

Users:
refers to all students, employees, contractors and volunteers using the Division network and IT assets.

Procedures:

1. Division-Owned Devices
    - 1.1. Data shall be stored in a secure manner and encrypted when transported on Division mobile devices.
    - 1.2. The Division Information and Security Officer, as directed by the Superintendent, has the right to monitor Division-owned devices and software and to retrieve information as required.
    - 1.3. Use of mobile devices is identified in the Student Responsible Technology Use Agreement (Form 140-1) and the Staff, Contractor, Volunteer Responsible Technology Use Agreement (Form 140-2).

1.4. Mobile devices shall be centrally managed by the Division Information and Security Officer to ensure compliance with Division security.
1.5. Users of mobile devices shall ensure stored data is regularly backed up (synced) on an EIPS-owned network and computer.
1.6. Division-owned mobile devices shall be passcode protected.
1.7. Loss of a Division-owned mobile device shall be reported as soon as possible to the Division Information and Security Officer. The Division Information and Security Officer will contact the Freedom of Information and Protection of Privacy (FOIP) Co-ordinator to assess the risk to the Division and determine appropriate action.
1.8. Lost mobile devices shall be deactivated and remotely erased where possible.
1.9. Mobile devices that have been deemed obsolete or are no longer in service shall be returned to the Division Information and Security Officer for removal of Division data.

2. Personally Owned Devices
   2.1. Employees and students shall be permitted to use their personal mobile devices in accordance with the following procedures:
      2.1.1. Users who have signed a Student Responsible Technology Use Agreement (Form 140-1) or a Staff, Contractor, Volunteer Responsible Technology Use Agreement (Form 140-2) will be able to use their mobile device to access the network with an assigned user ID.
      2.1.2. General internet connectivity of personal mobile devices may be available through the wireless network.
   2.2. The Division is not liable or responsible for any loss, theft or damage of personal mobile devices and Information Technologies shall not provide technical support for personal mobile devices.
   2.3. Private or confidential data shall only be stored on personal mobile devices when appropriate security and encryption requirements are met.
   2.4. The passcode feature must be enabled.

Reference:

Section 52, 53, 68, 196, 197, 222, 225 *Education Act*
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canada Criminal Code
Copyright Act
ATA Code of Professional Conduct