Administrative Procedure 141

PORTABLE TECHNOLOGY SECURITY

Background

All staff using Division information at a Division location or otherwise are responsible for the management and safekeeping of information under their control by ensuring that there is adequate security to prevent unauthorized access, collection, use, disclosure or disposal of information.

Sensitive and confidential information stored on portable technology such as laptops, personal organizers, cell phones or memory sticks must be kept to an even higher standard due to the higher risk of equipment theft.

Procedures

1. All employees will assist in protecting devices issued by Division and any Division data contained on them. Mobile devices are defined to include any device that is portable, such as netbooks, laptops, tablets, USB drives/sticks and cell phones. They are assigned and inventoried to specific users. Any change in the user assigned to a particular mobile device, must be reported to the Technology Department, other than USB drives/sticks which must be inventoried by the school or department.

2. Users are expressly forbidden from storing Division data on devices that are not owned by Division. All such data should be accessed only through a browser when using a non-Division device.

3. Mobile computing devices containing or accessing information resources must be supported by the Technology Department to connect over the private network. As well, all non-Division devices must access data through the public network.

4. Employee used and Division owned, portable computing devices and portable electronic storage media, must use encryption. Individuals are strongly encouraged to encrypt their own personal devices. Devices used only by students need not be encrypted.

5. Unless written approval has been obtained from the FOIP Coordinator, databases or portions thereof that reside on the network, will not be stored on any mobile computing or storage devices.

Reference: Section 60, 61, 113 School Act