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 password protection mechanisms available on portable technology must be activated and utilized consistently and to the greatest extent possible. Industry standards/methods are to be deployed in the selection of appropriate passwords.

2. All files containing sensitive or confidential information that are stored on portable technology must be encrypted.

3. Any information that is no longer required on portable technology is to be transferred immediately to more secure electronic storage.

4. All security measures adopted for other technology use within the Division apply to portable technology.

5. Staff are encouraged to use Remote Desktop to access sensitive or confidential information on Foothills School Division servers in the absence of local file encryption. In this way portable technology should not have any files with sensitive data stored locally on them.

Reference: Relevant Legislation & Regulations