PORTABLE TECHNOLOGY SECURITY

Background

All staff using District information at a District 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 loss or 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. Passwords should be treated in strict confidence and should not be shared with any other individual.
3. All files containing sensitive or confidential information that are stored on portable technology must be encrypted/password protected.
4. Any information that is no longer required on portable technology is to be transferred immediately to more secure electronic storage.
5. All security measures adopted for other technology use within the District apply to portable technology.

Reference: *Sections 17, 20, 22, 65, 85 School Act*
Freedom of Information and Protection of Privacy Act
School Regulation 265/89

SD No. 40 (New Westminster)

Adopted: May 30, 2017