Administrative Procedure 141

PROTECTION OF DISTRICT RECORDS

Background

The District recognizes that there may be circumstances in which it is necessary or reasonable for employees to perform employment responsibilities from locations outside of their assigned workplace. However, where the performance of such responsibilities requires employees to access or use personal information about students, staff, parents or other individuals from outside of the workplace or confidential information of the District, this poses increased risks to the security, privacy and confidentiality of this information.

The purpose of these procedures are to establish consistent and appropriate standards with respect to the use of remote technology by employees to access or store personal information related to District operations and to any other access, storage or removal of records containing personal or confidential information outside of the workplace.

Definitions

"**Act**" means the *Freedom of Information and Protection of Privacy Act,* and regulations thereto, as amended from time to time.

"Confidential Information" means all records containing information about the District that is not generally known, used or available to the public.

"**Information Security Classification System**" means a framework for classifying data adopted by the District from time to time.

"**Information Technology Department**" means the District's Information Technology Department.

"**Mobile Storage Devices"** means any portable electronic device that is used to store personal information, including lap top computers, flash drives, USB drives, external hard drives, smart phones and other similar devices.

"**Personal Information**" means "personal information" as defined in the Act that staff obtain or access in connection with their employment or engagement. The Act defines "personal information" as any information pertaining to an identifiable individual, excluding business contact information.

"**Sensitive Personal Information**" means personal information pertaining to: a student's educational performance; any person's medical or mental health or treatment;

educational or employment history or discipline records; financial and identity information (social insurance number, date of birth, driver's license number), and any other categories of information the inadvertent disclosure of which may give rise to a reasonable prospect of harm to the individual about whom the information pertains or information that has otherwise been designated as sensitive or requiring higher levels of security in accordance with the District's Information Security Classification System.

"**Records**" has the meaning set out in the Act, including all paper records, electronic records, photographs, recordings, or any other media or device upon which confidential information and/or personal information is recorded or stored.

"Manager" means the principal, manager or other supervisor who is responsible for the management of the operation or administration of a workplace.

"**Staff**" means the employees of the District and includes any independent contractors who have access to personal information in the course of carrying out their employment or contracted responsibilities.

"**Systems**" means the electronic information management system or network maintained and operated by the District for the purpose of storing and managing information collected, used or retained by it for the purposes of carrying out its duties and responsibilities as a Board under the *School Act* (BC).

"**Workplace**" or **"Worksite"** means the school, office or other District owned or operated site(s) at which the member of staff ordinarily carries out his/her employment responsibilities.

1. **Procedures**

1.1 The District recognizes that staff may from time to time carry out work related tasks outside of school hours and from locations outside of the workplace. Staff are expected to follow these procedures to ensure that they take reasonable precautions to ensure that such activities do not give rise to preventable risks of breaches of privacy occurring.

1.2 All staff are to be aware that the removal of District records from the workplace gives rise to risks that such information may be lost, stolen or accessed by unauthorized persons. Before materials containing personal information or confidential information are removed from the workplace, staff are to consider:

1.2.1 The purpose for doing so and whether the purpose could be achieved without taking such materials out of the workplace.

1.2.2 The safeguards that are in place to protect the information from unauthorized access, loss or theft.

1.2.3 The sensitivity of the information involved.

1.3 If it is necessary for staff to remove District records from the worksite, only the minimum amount of confidential and/or personal information required is to be removed.

1.4 If District records are removed from the workplace, staff members are to be conscious of what has been removed, and in appropriate cases, it may even be prudent for staff members to maintain a written record or inventory of what has been removed.

1.5 Staff are expected, wherever possible, to access District records through the secure use of the Systems rather than by saving such information to mobile storage devices, where it is prone to loss or theft or other unauthorized access.

1.6 Staff shall comply with the directives and standards issued from time to time by the Chief Officer of Information and Technology regarding the secure access and storage of District records on mobile storage devices and other devices, including in respect of the creation of secure passwords, encryption, storage and destruction.

1.7 The Chief Officer of Information and Technology shall review on at least an annual basis the information security systems in use within the District to ensure that District records are protected from loss, theft and unauthorized access, use or disclosure.

1.8 The manager at each workplace shall review these procedures with all members of staff at the commencement of each school year.

2. Physical Records

2.1 Consideration is to be given to whether copies rather than original records are to be used if they are to be removed from the workplace.

2.2 Records removed from the worksite are to remain in the possession of the staff member with the care and control of them and are not to be left unattended in a public location (including a parked vehicle). When not in the actual possession of the staff member, they are to be maintained in a secure location (e.g. a locked office or drawer within the staff member's home with limited access by persons other than the staff member) access to which is limited to the staff member.

2.3 It is important that staff members are conscious of any physical records that they remove from the workplace and ensure that they are returned to the workplace in a timely way.

2.4 Upon returning to the office, staff shall return original records to their original storage place as soon as possible and destroy copies securely.

3. Mobile Storage Devices

3.1 All staff are to be conscious that mobile storage devices can be easily lost, stolen or misplaced. The storage of District records on such devices therefore gives rise to an increased risk of harm and unauthorized access to confidential and/or personal information.

3.2 Mobile storage devices must be kept physically secure at all times, including by ensuring they are never left unattended in public locations (including a parked vehicle).

3.3 Mobile storage devices are to ordinarily be kept in the physical possession of the staff member having their care and control, and when not directly in that person's possession, are to be stored in a secure location (e.g. locked office or drawer in the staff member's home) access to which is limited to the staff member.

3.4 All mobile storage devices that are used to store District records, including laptops, flash drives, external hard drives, smart phones and other such technologies, must be protected at all times through the use of a secure password and, where possible, through the use of encryption.

3.5 Mobile storage devices containing District records are not to be shared with others, including family members or friends.

3.6 All files containing confidential and/or personal information that are saved to a mobile storage device must be encrypted.

3.7 Files containing sensitive personal information are not to be saved to a mobile storage device except as necessary to fulfill a specific identified purpose and are to be permanently deleted from the mobile storage device once that purpose has been satisfied.

3.8 Staff are expected to refrain generally from viewing confidential and/or personal information on a mobile storage device within public places, but if it is necessary to do so, staff are to ensure that the information cannot be viewed by unauthorized parties by taking appropriate precautions.

4. Remote Access to Systems and Email

4.1 Staff may not use personal email accounts as a means of transferring District records containing confidential and/or personal information.

4.2 Where personal information is transferred by facsimile, staff members shall ensure that any facsimile machine used to transmit the information is not in a public place and that access to it is limited. In the event that non-District personnel have access to such machines, the staff member shall ensure that any images of the documents transmitted that may be stored by the machine are permanently and securely destroyed.

4.3 The District maintains systems through which staff may be granted access privileges permitting remote access to District records. All staff members with such privileges shall comply with the directives issued from time to time by the Chief Officer of Information and Technology concerning securely accessing and using the Systems.

4.4 Staff wishing to utilize District Systems at home are to only do so using secure devices issued by the Information Systems and Technology Department.

4.5 At a minimum, staff members using the systems, shall ensure that they:

4.5.1 Log off the systems or shut down computers when not in use.

4.5.2 Follow the Chief Officer of Information and Technology defined protocol(s) for accessing the District systems through unsecured WIFI networks.

4.5.3 Set an automatic logoff to run after a minimum period of idleness.

4.5.4 Do not share the password for the systems with any other person, including coworkers.

4.6 Staff members may not save any files containing District collected personal information to their home or personal computers.

5. Loss, Theft and Unauthorized Access

5.1 All staff members are responsible to immediately make a report to “immediate supervisor/principal, supervisor/principal to report to immediate supervisor” in the event that they become aware of any loss, theft or other unauthorized access to District records.

Adopted: December 15, 2020