**SD 42 PROCEDURE: 5780.2**

**PROTECTION OF SCHOOL DISTRICT RECORDS WHEN WORKING AWAY FROM THE WORKPLACE**

---

## A. Introduction / Purpose

The Board of Education of School District No. 42 (Maple Ridge - Pitt Meadows) ("School District") recognizes that there may be circumstances in which it is necessary or reasonable for employees to perform employment responsibilities and access School District files and information from locations outside of their assigned workplace. However, accessing, using, or storing confidential information or the personal information of students, staff, parents or other individuals from outside of the workplace poses increased risks to the security, privacy and confidentiality of this information.

The purpose of this Procedure is to provide guidance and establish the expectation of Staff when working at locations out of the Workplace.

## B. 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 School District that is not generally known, used or available to the public;

"**Information Technology Department**" means the School 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 contractual responsibilities to the School District. The Act defines "personal information" as any information pertaining to an identifiable individual, excluding business contact information;

"**Sensitive Personal Information**" means Personal Information that due to nature or the context in which it is provided is inherently personal or intimate in nature and includes information such as student files, medical or mental health information, 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 unauthorized 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;

"**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 School District, and includes trustees and 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 School 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 of Education under the *School Act* (BC);

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

## C. General Principles

- The School District encourages Staff to access, use and store Personal Information at the Workplace and using the Systems. Removing Personal Information or Records or accessing them from remote locations exposes such materials to avoidable risk.

- The School 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 follow responsible practice for the protection of Personal Information, Confidential Information and Records.

- The removal of digital or physical 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 should consider:

    - The purpose for doing so and whether the purpose could be achieved without taking such materials out of the Workplace;

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

    - The sensitivity of the information involved.

- Staff members who have possession of Records at locations outside of the Workplace, are expected store and retain such materials only to the extent necessary to carry out their responsibilities to the School District.

- Staff who require access to electronic Records must, wherever possible, access such Records through secure access to the Systems rather than by saving such information to Mobile Storage Devices, where it is prone to loss or theft or other unauthorized access.

- Staff shall comply with the directives and standards issued from time to time by the Information Technology Department regarding remote working arrangements, including in relation to the security of passwords, login credentials and encryption keys; the secure use of virtual private networks and multi-factor authentication; storage of electronic Records on Mobile Storage Devices; and the secure destruction of Records.

- The Information Technology Department shall review on at least an annual basis the information security systems and arrangements for remote work in use within the School District to ensure that Records are protected from loss, theft and unauthorized access, use, disclosure and destruction.

- The Manager at each Workplace shall review this Procedure with all members of Staff at the commencement of each school year.

## D. Physical Records

- Original copies of paper files and Records must remain at the Workplace. To the extent possible, physical copies of Records should not be removed from the Workplace or reproduced or printed from offsite locations. Physical records that are removed from the Workplace or printed from offsite locations should be securely destroyed or returned to the Workplace as they are no longer needed.

- Physical Records when in the possession of the Staff member with the care and control of them, should not be left unattended in settings where they may be vulnerable to unauthorized access, theft or loss (including in all public or quasi-public spaces e.g. a parked vehicle). When not in the actual possession of the Staff member, they should 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).

## E. Mobile Storage Devices

- All Staff should be conscious that Mobile Storage Devices can be easily lost, stolen or misplaced. The storage of Records on such devices therefore gives rise to an increased risk of harm and unauthorized access to Confidential and/or Personal Information. Staff are therefore expected to exercise appropriate diligence when such devices are within their possession or control.

- Mobile Storage Devices on which Records are stored must be kept physically secure at all times, including by ensuring they are never left unattended in locations where they may be vulnerable to unauthorized access, theft or loss.

- Mobile Storage Devices should 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, should 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.

- All Mobile Storage Devices that are used to store 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.

- Mobile Storage Devices containing Records should not be shared with other non-Staff members, including family members or friends.

- Files containing Sensitive Personal Information should not be saved to a Mobile Storage Device except as necessary to fulfill a specific identified purpose and should be permanently deleted from the Mobile Storage Device once that purpose has been satisfied. All Records that contain or comprise Sensitive Personal Information must be encrypted when saved to a Mobile Storage Device.

- Staff are expected to refrain generally from viewing Confidential and/or Personal Information on Mobile Storage Devices where there is a risk of such materials being viewed or accessed by unauthorized parties.

## F. Remote Access to Systems and Email

- Staff may not use personal email accounts as a means of transferring Records.

- Staff wishing to utilize Systems at home should only do so using secure devices issued or approved by the Information Technology Department.

- At a minimum, Staff members using the Systems, shall ensure that they:

    - log off the Systems or shut down computers when not in use;

    - follow the Information Technology Department defined protocol(s) for accessing the school district Systems through unsecured Wi-Fi networks;

    - set an automatic logoff to run after a minimum period of idleness;

    - do not share the password for the Systems with any other person, including coworkers.

- Staff members may not save any files containing Records to personal computers or devices.

## G. Loss, Theft and Unauthorized Access

All Staff members are responsible to immediately make a report to the IT Help Desk in the event that they become aware of any loss, theft or other unauthorized access to school district records.

**UPDATED: September 2024**