AP 665 PROTECTION OF SCHOOL DISTRICT RECORDS WHEN AWAY FROM THE WORKPLACE

CARIBOO - CHILCOTIN SCHOOL DISTRICT

RATIONALE:

There may be circumstances where it is necessary or reasonable for staff to perform employment responsibilities from locations outside of their assigned workplace. However, where the performance of such responsibilities requires staff to access or use information about students, staff, caregivers or other individuals, or confidential information of the school district from outside of the workplace, there is an increased risk to the security, privacy, and confidentiality of the information.

PROCEDURE:

1. General

1.1 All staff should be aware that the removal of school district records from the workplace increases the risk 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:

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

1.1.2 the safeguards in place to protect the information from unauthorized access, loss, or theft; and

1.1.3 the sensitivity of the information involved.

1.2 If it is necessary for staff to remove school district records from the workplace, only the minimum amount of confidential and/or personal information required should be removed.

1.3 If school district records are removed from the workplace, staff should be conscious of what has been removed, and in appropriate cases, maintain a written record or inventory of what has been removed.

1.4 Staff are expected, wherever possible, to access school district records through the secure use of the district website, staff portal and computer systems rather than by saving such information to mobile storage devices, where it is prone to loss or theft or other unauthorized access.

1.5 Staff shall comply with the district's directives and standards regarding the secure access and storage of school district records on mobile storage devices and other devices, including the creation of secure passwords, encryption, storage, and destruction.

1.6 The District shall review, on at least an annual basis, the district's information security systems to ensure school district records are protected from loss, theft, and unauthorized access, use or disclosure.

1.7 The Principal/supervisor at each workplace shall review this procedure annually with all members of staff, no later than November of each school year.

2. Physical Needs

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

2.2 Records removed from the workplace should remain in the possession of the staff member who is responsible for their care and control of them at all times and should not be left unattended in a public location (including a parked vehicle). When not in the actual possession of staff, 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 employee).

2.3 It is important staff are conscious of any physical records they remove from the workplace and ensure they are returned by 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 should be aware that mobile storage devices can be easily lost, stolen, or misplaced. The storage of school district records on such devices gives rise to an increased risk of harm and unauthorized access to confidential and/or personal information.

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

3.3 Mobile storage devices should ordinarily be kept in the physical possession of the staff member who is responsible for 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.

3.4 All mobile storage devices used to store school district records, including laptops, flash drives, external hard drives, smartphones, 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 school district records should not be shared with others, including family members or friends.

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

3.7 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.

3.8 Staff are expected to refrain from viewing confidential and/or personal information on a mobile storage device within public places. If it is necessary, staff should ensure the information cannot be viewed by unauthorized parties.

4. Remote Access to Systems and Email

4.1 Staff may not use personal email accounts to transfer or save school district records containing confidential and/or personal information.

4.2 The school district maintains systems through which staff may be granted access privileges permitting remote access to school district records. All staff with such privileges shall comply with the directives issued by the school district concerning securely accessing and using the systems.

4.3 Staff wishing to utilize school district systems at home should only do so using secure devices issued by the school district.

4.4 At a minimum, staff using the systems shall ensure they:

4.4.1 log off the systems or shut down computers when not in use;

4.4.2 do not access the school district systems through unsecured Wi-Fi networks;

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

4.4.4 do not share the password for the systems with any other person, including coworkers.

4.5 Staff may not save any files containing school district-collected personal information to their home or personal computers.

5. Loss, Theft and Unauthorized Access

5.1 All staff are responsible for immediately reporting to their supervisor if they become aware of any loss, theft, or other unauthorized access to school district records.