AP 147 – Protection of School District Records When Working Away from the Workplace

Background:

The purpose of this Administrative Procedure is to establish consistent and appropriate standards with respect to the use of technology by staff members to access or store information related to School District operations; and the access, storage or removal of records (hardcopy or electronic) containing personal or confidential information outside of the workplace.

The Board of Education of School District No. 45 (West Vancouver) recognizes that there may be circumstances in which it is necessary or reasonable for staff members to perform employment responsibilities from locations outside of their assigned workplace. However, where the performance of such responsibilities requires staff members to access or use information about students, staff, parents 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.

Procedures:

1. General

1.1 All staff members 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 members 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;

1.2 If it is necessary for staff members 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 members should 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.

1.4 Staff members are expected, wherever possible, to access school district records through the secure use of the school district website 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 members shall comply with the directives and standards issued from time to time by the information technology department of the school district regarding the secure access and storage of school district records on mobile storage devices and other devices, including in respect of the creation of secure passwords, encryption, storage and destruction.

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

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

2. Physical Records

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 the 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 members, they should be maintained in a secure location (e.g. a locked office or drawer within the staff members' home, with limited access by persons other than the employee).

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 members 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 members should be conscious 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 kept physically secure at all times, including by ensuringthey 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 that are used to store school 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 school district records should not 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 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 members 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 members should ensure that the information cannot be viewed by unauthorized parties by taking appropriate precautions.

4. Remote Access to Systems and Email

4.1 Staff members may not use personal email accounts as a means of transferring school 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-school 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 school district maintains systems through which staff members may be granted access privileges permitting remote access to school district records. All staff members with such privileges shall comply with the directives issued from time to time by the information technology department concerning securely accessing and using the systems.

4.4 Staff members wishing to utilize school district systems at home should only do so using secure devices issued by the information technology department.

4.5 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 WiFi 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.

4.6 Staff members 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 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.

Legal Reference: *School Act, Freedom of Information and Protection of Privacy Act*