FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

Background

The District is a public body subject to the BC Freedom of Information and Protection of Privacy Act (FOIPPA). This statute contains provisions that regulate the public's access to information held by the District and govern the District's responsibilities to protect personal information from unauthorized access, use or disclosure. The District must ensure all personal information held in its custody and control is protected by reasonable security arrangements.

As the custodians of both student and employee personal information, the District has the legal obligation to safeguard the confidentiality of personal information pertaining to private individuals. Personal information may only be obtained as authorized by FOIPPA and used for the specific purposes for which it is gathered. The management and safekeeping of such information is the responsibility of each designated employee. The Secretary Treasurer is the District Privacy Officer and will monitor this Administrative Procedure.

Definitions

Contact Information – Under FOIPPA, contact information means information enabling an employee to be contacted at work and includes the name, position, business contact number, business address and business email.

Employee Personal Information – Under FOIPPA, employee personal information means any recorded information about an identifiable employee (see personal information below) other than contact information. The release and sharing of contact information is not a privacy violation.

Personal Information – Under FOIPPA, personal information means any information about an identifiable individual. Personal information may include data such as unique identifiers (PEN/SIN), school records, contact numbers, gender, medical history, education, employment, behavioral assessments, personnel evaluations, digital images, audio and video recordings, racial or ethnic origin, sexual orientation or religious beliefs.

Student Personal Information – Under FOIPPA, student personal information includes personal information (as defined above) plus any information that identifies a student including the student's full name, address, and contact numbers, PEN (personal education number), assessments, results, and educational records. District employees may disclose student personal information to other District employees where such disclosure is necessary for the performance of the duties of the employee and to other Districts where it is necessary for educational purposes.

Procedures

1. Collection of Personal Information

    1.1. Employees will be directly notified of this Administrative Procedure.

1.2. The District has the legal authority to collect personal information that relates directly to and is necessary for its operating programs or activities or as reasonably required to establish, maintain, manage or terminate an employment relationship without consent assuming employees have been notified of the collection of information. Personal information will be collected directly from the individual the information is about; other methods of collection may be indirectly used as governed by FOIPPA.

1.3. Other methods of collection may include, but not limited to, GPS or video surveillance. GPS is used by the District to track assets and may on occasion be used to locate employees as cell phones are not provided for contact. Video surveillance is used for asset, student and employee safety. Indirect collection methods may be used if a student or employee comes under investigation; all use will follow FOIPPA.

1.4. When a Principal or the District collects personal information about students or families, parents are to be informed of the purpose for which the information is being collected. The parents of a student must authorize the disclosure of personal information for purposes ancillary to educational programs such as:

1.4.1. Newsletter publications;

1.4.2. Website posting;

1.4.3. Video conferencing;

1.4.4. Social media applications;

1.4.5. Honour roll lists;

1.4.6. Team rosters; or

1.4.7. Yearbooks

1.5. Parents will complete and submit Form 180-1 Parental Consent upon their child's initial enrolment. Where the parent provides consent, this will allow the Principal or District to publish student personal information for purposes such as:

1.5.1. Recognition of achievement;

1.5.2. Promotion of events; or

1.5.3. Commemoration of school events.

1.6. The authorization given above is deemed in effect until the student changes or transitions to another school. Parents will have the ability to opt out of providing information that is not directly related to a student's educational program or necessary for the District's operational activities.

2. Use of Personal Information

2.1. Personal information will be used for the purpose for which it is collected or for a use consistent with that purpose. When there is a need to access information for a purpose other than why it was collected or if there is uncertainty as to the confidentiality of the information, clarification will be provided from the District Privacy Officer.

3. Disclosure of Personal Information

    3.1. Personal information may be disclosed to an external or third party if the individual who is the subject of the information has provided written consent. In the case of a student under age 19, such consent may be provided by the student's parent. Disclosure of personal information is not to occur when using a mobile phone or in any physical location that may compromise confidentiality.

4. Access to Personal Information

    4.1. Employees of the District have a general right of access to any record in the custody or under the control of the District, provided that access is required to complete the duties of the work assignment.

    4.2. A parent has the right to access personal information on behalf of a child under the age of 19.

    4.3. The District governs the right of access by an individual to his/her own personal information and by the public to any information or records in its custody or control of the District. Districts, other government ministries or law enforcement agencies may have access to personal information where obtaining this information is necessary for the provision of their services.

5. Securing Personal Information

    5.1. Information management must be dealt with in a responsible, efficient, ethical and legal manner. Users of electronic network resources are not to disseminate personal information to anyone not covered by a confidentiality agreement; additionally, precautions are to be taken to ensure information is protected from unauthorized access, use and disclosure. All District employees are expected to maintain, secure and retain appropriate student and personnel records in a manner that respects the privacy of employees, students and students' families and complies with the regulations specified in FOIPPA.

    5.2. The following safeguards, though not an exhaustive list, will assist in protecting privacy of personal information for both students and employees:

        5.2.1. Security (e.g.: passwords, encryption) must be in place for personal information, stored, printed or transferred by computers;

        5.2.2. All electronic mobile devices (even personally owned devices) that access or store District data must be secured by a password logon and use the highest available encryption options;

        5.2.3. All electronic mobile devices that contain or can access District data are to be kept on one's person and never be left unattended in public areas (e.g.: classrooms, hotel rooms);

        5.2.4. Passwords are not to be shared nor is anyone to logon to a system using an ID that has not been specifically assigned to them; and

        5.2.5. Paper files are to be safeguarded by implementing reasonable security precautions such as, locked storage, removal of personal information from work areas, and shredding of documents containing personal information.

    5.3. Access to any personal information is to be based on employment duties requiring such access. Unauthorized access to information about colleagues, friends, or family is not

permitted. Any personal information that is no longer required for administrative, financial or legal purposes will be destroyed in a confidential manner. Paper files due for destruction are to be securely shredded and disposed of; computer files are to be deleted in their entirety; any data storage devises are to be fully erased prior to disposal.

6. Investigation of Complaints

6.1. Anyone suspecting or aware of the unauthorized collection, use, access, or disclosure of student or employee personal information, breach of confidentiality protocols or contraventions of this Administrative Procedure must report such activities to the District Privacy Officer (Secretary Treasurer).

Reference: Sections 22, 65, 85 School Act
Freedom of Information and Protection of Privacy Act
Freedom of Information and Protection of Privacy Regulation

Adopted: November 2019
Revised: