

611 Privacy

Adopted: November 22, 2005

Policy

Guiding Principles

The Board of School Trustees, School District 44 (North Vancouver) (the “District”) is a public body subject to the *Freedom of Information and Protection of Privacy Act (FOIPPA)* and the *School Act*. Both statutes contain provisions that address privacy of personal information held by the District.

As the custodian of both student and employee personal information, the District has a legal obligation to protect personal information in its custody or control from unauthorized access, use, disclosure, and disposal. In fulfilling these responsibilities, the District complies with the provisions of the *FOIPPA* and the *School Act* that apply to records in its custody or control.

The District will provide information to employees, volunteers and service providers about this Policy and the need to protect the personal information of employees and students in compliance with this Policy. In the event an employee is uncertain about whether information is confidential or the nature or extent of his or her obligations under this Policy, the employee must seek clarification from the District Privacy Officer.

FOIPPA

The *FOIPPA* governs the collection, use and disclosure of personal information by the District and requires that personal information held in the District’s custody and control be protected by reasonable security arrangements.

Under the *FOIPPA* “personal information” means any information about an identifiable individual. Personal information may include data such as unique identifiers (PEN/SIN), school records, residential phone numbers, gender, aboriginal status, medical, educational, employment, or psychiatric history, behavioural assessments, personnel evaluations, racial or ethnic origin, sexual orientation or religious beliefs.

Collection of Personal Information

In accordance with the *FOIPPA*, 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 otherwise authorized by statute. Personal information will be collected directly from the individual the information is about unless another method of collection is authorized by the individual or the Act.

Use of Personal Information

Personal information will be used for the purpose for which it was collected or for a use consistent with that purpose. Additional authorized uses are identified in Part 3 of the *FOIPPA*.

Disclosure of Personal Information

Disclosure of personal information occurs when the information is provided to an external or third party. Such disclosure must comply with the provisions of Part 3 of the *FOIPPA*.

Personal information may be disclosed to a third party if the individual who is the subject of the information has provided written consent in accordance with the *FOIPPA* Regulation. In the case of a student under age nineteen, such consent may be provided by the student's parent or guardian.

Access to Personal Information

The *FOIPPA* provides a general right of access to any record in the custody or under the control of a public body, including records containing personal information, subject to certain exceptions which are set out in Part 2 of the Act.

The *FOIPPA* Regulation allows a parent or guardian to access personal information on behalf of a child under the age of nineteen.

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 in accordance with *FOIPPA* and the *School Act*.

School Act

The *School Act* addresses privacy in the context of student records (79). "Student record" is defined in Section 1 of the *School Act*. Appropriate procedures must be in place for the storage, retrieval, and appropriate use of student records and the District must ensure the confidentiality of information contained in student records.

All student records are the property of the District. A student and parent or guardian has a right of access to copies of academic records and other student records (9), as well as information about the student's progress, attendance and behavior at school (7). Under the *School Act*, records that are in the sole possession of the maker are not part of the official student file. Please refer to *Policy 601: Access to Student Records*.

Student Personal Information

Student personal information includes any information that identifies a student including the student's name, address, and telephone number, 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 school districts where it is necessary for educational purposes.

In accordance with the *FOIPPA*, other ministries, school districts, or law enforcement agencies may have access to personal information where this is necessary for the provision of their services.

If student personal information is intended to be used for purposes ancillary to educational programs such as newsletter publications, website postings, honor roll lists, team rosters or yearbooks, students and/or parents must authorize the disclosure of personal information for such purposes. When a school or the District collects personal information about students or families, parents/guardians should be informed of the purpose for which the information is being collected.

Parents/guardians will be provided with a form entitled *Authorization for Disclosure of Student Personal Information* upon their child's initial enrollment. Where the parent or guardian provides consent, this will allow the school or the District to publish student personal information for purposes such as recognition of achievement, promotion of events, or commemoration of school events. This authorization will be sought annually at the beginning of each school year. Parents/guardians 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.

Employee Personal Information

Employee personal information is any recorded information about an identifiable employee other than contact information. "Contact information" means information enabling an employee to be contacted at work and includes the name, position name, business telephone number, business address, business email, and fax number.

The collection, use, disclosure, access to and disposal of employee personal information are governed by the *FOIPPA*. All provisions of the *FOIPPA* that apply to employee personal information in the District's custody or control will be observed.

Securing Personal Information

In an organization with province wide electronic data management systems such as BCeSIS, unique privacy concerns exist. Information management must be dealt with in a responsible, efficient, ethical and legal manner. Users of computer network resources should not disseminate personal information to anyone not covered by a confidentiality agreement, and even then, precautions should 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.

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

- Security (e.g. passwords, encryption) must be in place for personal information, stored, printed or transferred by computers and electronic mobile devices.
- Paper files due for destruction should be securely shredded and disposed of; computer files should be erased in their entirety.
- Information should be safeguarded by implementing reasonable security precautions: locked storage; removal of personal information from work areas; proper shredding of binned material.
- Confidential warning should be listed on fax cover sheets to prevent information from being accessed and viewed by an unauthorized party if a fax is obtained in error. Highly sensitive material should not be faxed.
- Personal information about a third party should be emailed only to authorized recipients. Emails sent or received with such personal information should be deleted immediately.
- Sensitive information such as pictures of students or employees, or personal information such as home addresses and phone numbers should not be transmitted or exposed on Internet or published without consent.
- Access by employees to personal information should be based on a need to know principle and where employment duties require such access. Unauthorized access to information about colleagues, friends, or family is not permitted.
- Any personal information of an employee that is no longer required for administrative, financial or legal purposes will be destroyed in a confidential manner.
- Internet/internal computer network systems must be used in accordance with protocols of *Communication Systems Policy 609*. Appropriate measures will be taken by the Manager of Information Technology Services to ensure security, restriction, and monitoring of processes.
- Laptops and other electronic devices, such as Personal Digital Assistants, should be either kept on one's person or be secured in safe physical storage.

- Passwords should not be shared with coworkers, nor should coworkers log in with another employee's password.
- Personal information should not be discussed in any physical location that may compromise confidentiality.
- Posting of personal information such as exam results should not contain student identifiers.

Publication of Policy

This Policy will be made available to all employee groups and volunteers. All employees and volunteers should familiarize themselves with the privacy obligations outlined in this Policy. Review of the policy will be undertaken if legislation necessitates changes.

Investigation of Complaints

The District has the right to investigate complaints or suspected contraventions of this Policy and may access files where misuse or misconduct is suspected. Other school districts or provincial authorities may assist in any investigation of privacy issues.

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 Policy must report such activities to the District Privacy Officer.

District Privacy Officer

The District Privacy Officer is the Secretary Treasurer who may be contacted at the North Vancouver School Board office, 721 Chesterfield Avenue, North Vancouver, BC.