This document provides an overview of FIPPA and outlines some important provisions related to managing personal information. However, it is not intended to be a substitute for legal advice.

FIPPA Overview

Public bodies in B.C., including school districts, are legally required to follow the provisions of the ***Freedom of Information and Protection of Privacy Act*** (FIPPA). This act defines the appropriate collection, use, disclosure, protection and storage of personal information.

"Personal information" comprises all recorded information about an identifiable individual. Learn more about personal information in the Personal Information Overview document. (https://bcerac.ca/wp-content/uploads/2019/04/Personal-Information-2019-04-25.pdf)

FIPPA is available online at: http://www.bclaws.ca/civix/document/id/complete/statreg/96165_00

Below you will find important sections of FIPPA for school districts to understand, accompanied by examples.

Collection of Personal Information

FIPPA describes the appropriate purposes and ways that personal information can be collected by public bodies such as school districts.

Authority:

To collect personal information under FIPPA, school districts need to have the necessary legal authority. When collecting information that is needed to carry out an initiative within a school district, **section 26 (c) of FIPPA** provides the necessary authority.

- *26 A public body may collect personal information only if:*

  (c) the information relates directly to and is necessary for a program or activity of the public body,

Example: A school district is implementing a new student information management system. To create profiles for each student, the district collects the first and last names and email addresses of students. In this case, the collection of this personal information is necessary for the program.

Notification:

School districts that are collecting personal information should also provide the necessary notification to students, parents or other individuals from whom personal information is being collected. **Section 27 (2) of FIPPA** provides direction about this type of notification.

- *27 (2) A public body must ensure that an individual from whom it collects personal information is told*

  (a) the purpose for collecting it,

  (b) the legal authority for collecting it, and

  (c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Example: Before creating user accounts for students in a new, educational software program, a school district sends a letter of intent to parents about the program and includes the following privacy notification.

Privacy Notification: Your child's first and last name and email address are being collected under the authority of Section 26 (c) of the *Freedom of Information and Protection of Privacy Act (FIPPA)*. This information will be used to create a user account for your child to access Learning Lab, a new online software program being used in classrooms. Questions about the collection of this information may be directed to our district's privacy officer:

Jane Smith
604-555-5555
Jane.Smith@schooldistrict.ca
School District Head Office
555 Johnson Road, Vancouver, BC.

Use of Personal Information

Section 32 of FIPPA explains how school districts can use personal information that they have collected appropriately. Specifically, **sections 32 (a) and (b)** state:

- *32 A public body may use personal information in its custody or under its control only*

  (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),

  (b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use

Example: If a school district collects the names and email address of students to create user accounts in a program called "Learning Lab", the district should not use this information to create user accounts in other software programs, as this would be a different purpose.

Disclosure of Personal Information

Section 33 of FIPPA and its three subsections describe various situations in which school districts could disclose personal information in their custody.

- *33 A public body may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3.*

Example: A school district's attendance management software experiences an outage, and they need to request technical support from an external service provider to restore the program. This technical support process may involve the disclosure of personal information stored within the software and under the control of the district. This disclosure is permissible under **subsections 33.1 (1) (p):**

- *33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:*

(p)the disclosure

(i) is necessary for

(A) installing, implementing, maintaining, repairing, trouble shooting or upgrading an electronic system or equipment that includes an electronic system, or

(B) data recovery that is being undertaken following failure of an electronic system that is sued in Canada by the public body or by a service provider for the purposes of providing services to a public body, and

(ii) in the case of disclosure outside Canada,

(A) is limited to temporary access and storage for the minimum tie necessary for that purpose, and

(B) in relation to data recovery under subparagraph (i)(B), is limited to access and storage only after the system failure has occurred

Protection of Personal Information

FIPPA, **section 30** requires school districts to protect personal information that is collected from students, parents, teachers, staff and others. This includes having technical and physical security measures, as well as policies and procedures, in place.

- *30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

Examples: Technical security measures could include resetting computer passwords on a regular basis or using anti-virus software to protect school computers.

Physical security measures could include always locking doors to server or file rooms in schools and ensuring that documents with personal information are not left in plain view on desks or photocopiers.

Procedure and policy measures could include raising awareness of staff and students through ongoing education strategies, and incorporating privacy best practices into day-to-day work and learning.

Storage of Personal information

Section 30.1 of FIPPA states that public bodies, which includes school districts, must not store personal information, or allow it to be accessed, outside of Canada. This is important to consider when looking at software programs and services that may collect and store personal information about users in the United States or other jurisdictions.

There are limited circumstances where storage and access outside of Canada are permissible, and these are stated in detail in **section 33.1 of FIPPA.**

- *30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:*

  (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;
  (b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;
  (c) if it was disclosed under section 33.1 (1) (i.1).

Example: A district wishes to use a new educational video streaming platform. Although the content is relevant to students in B.C., personal user data is stored on servers outside of Canada. In this case, the district must seek consent from students or their parents/guardians to have their personal information stored outside of Canada. Consent cannot be forced.

Questions?

If you have specific questions about FIPPA, contact the privacy officer in your district or the provincial privacy helpline.

Email: privacy.helpline@gov.bc.ca
Phone: 250-356-1851, or 1-800-663-7867 (and ask for the Privacy and Access Helpline).