FOCUSED
EDUCATION RESOURCES

PMP Concepts and Terminology

WHAT IS A "PUBLIC BODY"?

FIPPA is provincial personal information protection legislation that applies only to "public bodies". The term "public body" is defined in **Schedule 1** of the Act and includes public school districts. Schedule 1 also sets out a lengthy list of other provincial government organizations and public sector institutions to which the Act applies, including ministries, municipal governments, health authorities, colleges and universities, professional regulatory bodies and government corporations.

WHAT IS THE MEANING OF "PERSONAL INFORMATION"?

"**Personal information**" is broadly defined in the Act as comprising any information about an identifiable individual, but it does not include a person's business contact information. Courts and decision-makers have long held that the concept of what is "personal information" is intentionally broad.

WHO IS THE "HEAD" OF A PUBLIC BODY?

Throughout FIPPA, there are provisions that indicate that the Head of a public body is the person who must make certain decisions. The Head of the school district for the purposes of FIPPA is a person that the Board of Education has designated as the Head and is typically the school district's Superintendent, Secretary-Treasurer or another member of senior management. The Head has the power to delegate some of their responsibilities to other officers or employees within the school district.

The designation of the Head should be documented in the school district's bylaws or in the form of a Board Resolution. Section 77 of FIPPA sets out the process for designating the Head of the school district for the purposes of FIPPA.

> **FIPPA, section 77**
>
> *A local public body, by bylaw or other legal instrument by which the local public body acts,*
>
> *a. must designate a person or group of persons as the head of the local public body for the purposes of this Act.*

WHAT CONSTITUTES CONSENT?

FIPPA does not require that individuals consent to every collection, use or disclosure of their personal information. Generally speaking, consent is not necessary where the Act already provides a public body with authority (see sections **26**, **27**, **32**, **33** and **34**). For example, consent is not required if:

- The school district is collecting and using personal information for purposes that are directly related to and necessary for its programs or activities (ss. 26(c), 32(a) and 34); or
- The school district is collecting information that is necessary to allow it to plan or evaluate its programs or activities (ss. 26(e), 32(a) and 34).

However, in some circumstances, school districts may wish to seek consent from staff, parents or students. For example, if the collection, use and disclosure of personal information is optional then seeking consent may be appropriate. Also, if FIPPA provides no clear authority to disclose personal

information, then consent may need to be sought. Consent may also be sought in circumstances where the use or disclosure of personal information is desirable, but not necessary.

An effective consent under FIPPA is one that is fully informed and is given voluntarily. This means that the individual providing the consent must understand the purposes for which the consent is sought, the consequences of providing or not providing the consent, and they must provide the consent voluntarily and without duress. It is also good practice to notify individuals how they can withdraw consent should they wish to do so.

Consent under FIPPA must be specific and in writing. Consent forms should be written in plain language to ensure that the reader clearly understands the applicability of the consent. A valid written consent should identify:

- The personal information the consent applies to.
- The date on which the consent is effective and when it expires (if applicable).
- Who may collect the personal information.
- The purposes for the collection, use or disclosure.
- How the personal information will be used.
- To whom the personal information will be disclosed.
- The jurisdiction where the personal information may be disclosed.

RESOURCES

The OIPC guide **Obtaining Meaningful Consent** provides additional information on this subject.

MINORS AND CONSENT

It is generally good practice to ensure that parents receive notice of the ways in which student information is collected, used, and disclosed by the school district. In some cases, it may also be prudent to obtain parental consent for a particular use or disclosure of personal information such as where student personal information is being shared with third parties.

A parent or legal guardian has the authority to provide consent on behalf of their minor child under FIPPA, but a parent's authority to do so is limited in two ways:

- The student must lack the capacity to give consent on their own; and
- The parent must be acting on behalf of the minor and not out of their own personal interests.

A student has the "capacity" to give consent when they have sufficient maturity and understanding to be able to comprehend the nature of the consent and the consequences of providing it. Generally speaking, students are thought to reach this level of maturity at around age 12 or 13, but the school district should make its own assessment in every case.

If a student has "capacity", then they should be a signatory to any privacy consent involving their personal information. In appropriate circumstances, the school district may still seek written authorization from the parent, but the "consent" itself must be given by the student.

HOW SHOULD WE SECURE PERSONAL INFORMATION?

Section 30 of FIPPA requires districts to implement "reasonable security measures" to protect the **personal information** in their custody or control. This includes taking all reasonable physical, technical, and administrative measures to protect personal information.

Protecting personal information is complex because it takes many forms and is disbursed throughout the organization.

The OIPC has published **Securing Personal Information: a self assessment for public bodies and organizations** (OIPC) to assist public organizations in understanding how and where internal security controls are recommended.

RESOURCES

- **Reasonable Security Measures for Personal Information Disclosures Outside of Canada** (OIPC)
- **Tips for Public Bodies and Organizations Setting Up Remote Workspaces** (OIPC).