FOCUSED
EDUCATION RESOURCES

Privacy Principles in Canada

All Canadian privacy laws are based on certain fundamental principles.

PRINCIPLE 1 - ESTABLISH ACCOUNTABILITY

Accountability refers to the principle that organizations are responsible for the personal information within their control. An organization demonstrates this accountability by developing policies and practices for handling personal information and by designating a Privacy Officer who can communicate, answer questions and respond to privacy concerns expressed by members of the community.

The accountability principle is reflected in section 36.2 of the Act, which requires all public bodies to implement a Privacy Management Program.

FIPPA, section 36.2

The head of a public body must develop a privacy management program for the public body and must do so in accordance with the directions of the minister responsible for this Act.

PRINCIPLE 2 - IDENTIFY THE PURPOSES

Organizations should strive to be transparent with individuals about the purposes for which they collect, use and disclose personal information. This means that when personal information is collected the individual should be told the purposes for collecting it and how it will be used. Organizations should also ensure that the purposes for collecting personal information are reasonable and are related to the public body's authorized programs and activities.

Generally, individuals should be provided with notice of the purpose for collecting information, the legal authority for collecting it, and the contact information of a district contact who can answer questions about the collection.

The obligation to notify appears in section 27(2) of the Act. Certain exceptions to the notice obligation are listed in section 27(3).

FIPPA, section 27(2)

1. *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 contact information of an officer or employee of the public body who can answer the individual's questions about the collection.*

PRINCIPLE 3 - OBTAIN CONSENT OR VERIFY AUTHORITY

All collection, use and disclosure of personal information must be authorized by FIPPA or may be the subject of individual consent. In the ordinary course, this means that the collection of personal information should be directly related to and necessary for a public body's authorized program or activities. FIPPA also authorizes the collection, use and disclosure of personal information in other circumstances, such as for law enforcement purposes and to plan and evaluate a public body's programs or activities.

Privacy Officers and those who make disclosure decisions within an organization should be familiar with the circumstances in which FIPPA permits the collection, use and disclosure of personal information.

The purposes for which personal information may be collected by public bodies appear in section 26 of the Act, which provides in part as follows.

FIPPA, section 26

A public body may collect personal information only if

- *a. the collection of the information is expressly authorized under an Act,*
- *b. the information is collected for the purposes of law enforcement,*
- *c. the information relates directly to and is necessary for a program or activity of the public body,*
- *d. with respect to personal information collected for a prescribed purpose,*
  - *i. the individual the information is about has consented in the prescribed manner to that collection, and*
  - *ii. a reasonable person would consider that collection appropriate in the circumstances,*
- *e. the information is necessary for the purposes of planning or evaluating a program or activity of a public body,*
- *f. the information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur,*
- *g. the information is collected by observation at a presentation, ceremony, performance, sports meet or similar event*
  - *i. at which the individual voluntarily appears, and*
  - *ii. that is open to the public, or*
- *h. the information is personal information that is collected by*
  - *i. a provincial identity information provider and the collection of the information is necessary to enable the provincial identity information services provider to provide services under section 69.2, or*
  - *ii. a public body from a provincial identity services provider and the collection of information is necessary to enable*
    - *A. the public body to identify an individual for the purpose of providing a service to the individual, or*
    - *B. the provincial identity information services provider to provide services under section 69.2.*

The circumstances in which a public body is authorized to use and disclose personal information are set out in sections **32**, **33** and **34** of FIPPA. Obtaining express written consent from affected individuals is one of the methods of ensuring that personal information may be used and disclosed, but FIPPA also provides for the use and disclosure of personal information without consent.

PRINCIPLE 4 - LIMIT COLLECTION

Public bodies should not collect more personal information than they need for an identified purpose. Personal information should also generally be collected directly from the individual the personal information is about, unless a method of indirect collection is authorized under the Act.

The obligation to collect personal information directly from the individual appears in **section 27(1)** of the Act, which also sets out the circumstances in which personal information does not need to be collected directly from the individual.

PRINCIPLE 5 - LIMIT USE, DISCLOSURE AND RETENTION

The use, disclosure and retention of personal information should also be limited to what is needed to fulfil the purposes for collecting it. If personal information is collected for one purpose, and the public body later wishes to use it for a different purpose, then the public body should ensure that FIPPA authorizes this use. The public body may also need to seek additional consent before using personal information for a different purpose.

It is also important that public bodies securely destroy personal information when it is no longer needed for administrative, operational or legal purposes.

PRINCIPLE 6 - BE ACCURATE

FIPPA requires public bodies to ensure that the personal information that they collect is accurate and complete. It is particularly important when personal information will be used to make decisions about an individual.

This obligation appears in section 28 of FIPPA:

> **FIPPA, section 28**
>
> *If:*
>
> *a. an individual's personal information is in the custody or under the control of a public body, and*
> *b. the personal information will be used by or on behalf of the public body to make a decision that directly affects the individual,*
>
> *the public body must make every reasonable effort to ensure that the personal information is accurate and complete.*

PRINCIPLE 7 - USE APPROPRIATE SAFEGUARDS

To comply with this principle, organizations are expected to make reasonable security arrangements to protect personal information under a public body's control. This includes employing physical measures, technical or electronic controls and organizational methods. What will be considered "reasonable" will depend on the circumstances, and security measures should be proportionate to the **sensitivity of the personal information** and the harm that may flow from unauthorized disclosure.

This obligation appears in section 30 of FIPPA, which provides:

> **FIPPA, section 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 collection, use, disclosure or disposal.*

The use of the word "reasonable" in section 30 indicates that the assessment of what is sufficient depends on the circumstances, and will be made on an objective basis. Generally, the more **sensitive** the information involved, the more robust the standards of security should be.

PRINCIPLE 8 - BE OPEN AND TRANSPARENT

To comply with this principle, organizations should ensure that they make information available to the community about their privacy management practices. This includes providing contact information for a Privacy Officer or other individual who can answer questions about personal information. Developing policies and procedures is also one of the ways that organizations satisfy this principle.

PRINCIPLE 9 - FACILITATE ACCESS TO PERSONAL INFORMATION

Individuals are presumptively entitled to be informed of the existence, use and disclosure of their personal information that is within the control of the school district. The school district should make every reasonable effort to facilitate an individual's right of access to their own personal information, including by responding to requests for access to information made under **Part 2** of the Act. Complying with this obligation also includes having processes in place to receive and respond to access requests as well as questions and concerns about personal information.

PRINCIPLE 10 - BE RESPONSIVE TO PRIVACY CONCERNS

Complying with this principle requires the school district to establish and follow processes that allow individuals and community members to raise concerns about whether the school district is complying with its privacy obligations under the Act and under its own policies.