The Personal Information Protection and Electronic Documents Act (PIPEDA) and its Application to Universities

A Communication Guide

The Council of Ontario Universities and the Associations of Universities and Colleges of Canada have jointly obtained a comprehensive legal opinion on behalf of their members. This document summarizes some of the key issues raised by the opinion. For further information, please contact the individual at your university who is responsible for privacy policy.

What is PIPEDA?

PIPEDA was enacted by the federal government to promote and enforce a unified privacy principle across Canada. It became law for federally regulated organizations (e.g., inter-provincial transport companies, banks, etc.) in January of 2001 and, as of January 1, 2004, most other organizations will also be required to comply.

PIPEDA holds organizations accountable for certain personal information in their custody and under their control. It requires that reasonable limits be placed on the collection, use, disclosure and retention of the personal information. In addition, PIPEDA requires openness with regard to an organization's policies and practices and free access to regulated personal information.

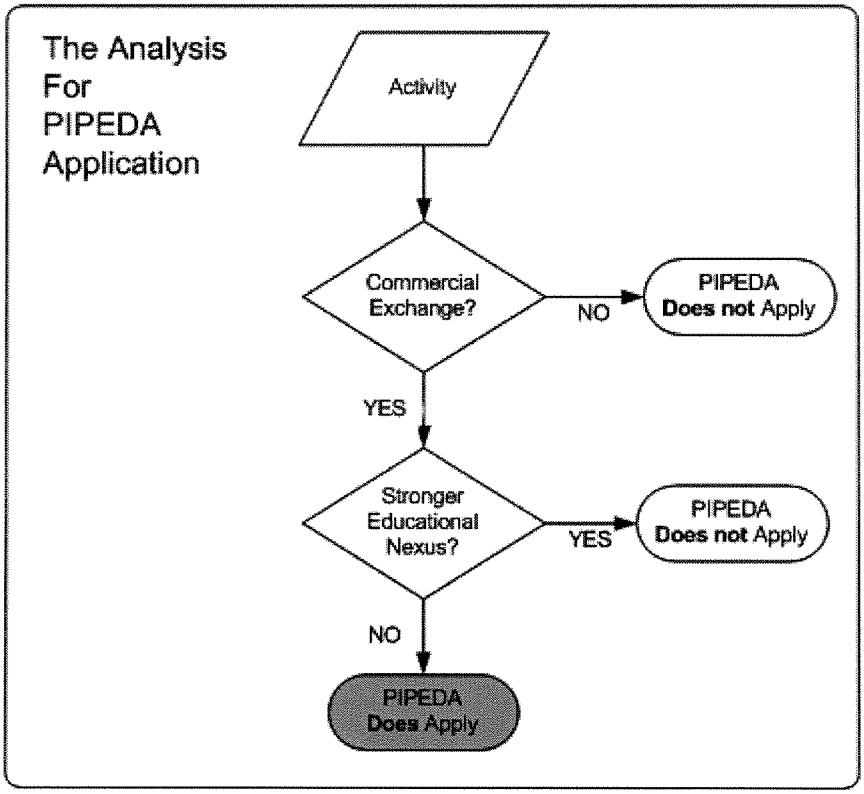
How does it apply to Universities?

PIPEDA applies to the collection, use, and disclosure of personal information in the course of "commercial activity." Obviously, its application to university educational activity is limited, but there will undoubtedly be some activities undertaken by every university that are "commercial" regulated by PIPEDA.

Examples of Activity Likely to be Excluded as "Educational"	Examples of Activity Likely to be Included as "Commercial"
-building and maintaining a student record to evaluate whether degree requirements are met	-collecting customer information at a university bookstore -using a former student's record to market goods and services to the former student

There are probably activities at every university that are partly educational in purpose and partly commercial in purpose, but are more difficult to characterize than those activities noted above.

Although it is not yet clear how the Privacy Commission and the courts will examine university activities to determine if they are regulated by PIPEDA, we believe university activities involving a "commercial exchange" (i.e., the sale or purchase of goods or services) and a dominant commercial (rather than educational) nexus will likely be subject to PIPEDA.



If you are uncertain about whether an activity is regulated by PIPEDA you should contact the individual responsible for privacy policy at your university. And if in doubt, the most prudent course of action is to treat the activity as regulated by PIPEDA.

Does every university department, school and faculty have some responsibility?

Yes. The responsibility is first and foremost to determine the scope of application of PIPEDA to personal information that is collected, used, or disclosed in your department. The next responsibility will be to ensure compliance with PIPEDA where it is required.

What do we do to comply with PIPEDA?

All universities must comply with the 10 PIPEDA Principles for managing personal information:

The 10 PIPEDA Principles	
1. Accountability 2. Identifying Purposes 3. Consent 4. Limiting Collection 5. Limiting Use, Disclosure and Retention	6. Accuracy 7. Safeguards 8. Openness 9. Individual Access 10. Challenging Compliance
http://www.privcom.gc.ca	

These principles require your university to delegate formal responsibility for creating and administering privacy policy, ensuring that privacy policy is openly communicated, administering requests for access to personal information, and administering privacy complaints. Once your university has created a privacy office, it will be your primary source of information on how to comply with PIPEDA.

How does it change the way we treat personal information?

If the information is not "personal information" used in the course of "commercial activity" you do not have to change the way you treat the information to comply with PIPEDA. However, if you "collect, use, or disclose" personal information in the course of "commercial activity" you must adhere to the 10 PIPEDA principles in treating that information.

The most important PIPEDA principle is the Consent Principle. You may only collect, use, or disclose an individual's personal information in the course of commercial activity with consent.

Consent can be implied when reasonable, but in many situations you may wish to obtain express consent to collect, use and disclose someone's personal information, especially when the information is of a sensitive nature. In order for consent to be valid, the individual consenting must be informed of your purpose – how you will use the information and to whom the information will be disclosed.

Key PIPEDA Concepts

Disclosure
Disclosure refers to the transfer of personal information to another organization that is not acting as agent. PIPEDA requires consent to disclose personal information in the course of commercial activity.

Although the exact rules are not yet clear, intra-organization information transfers should not require consent. Similarly, transfer to an agent (e.g. an organization that mails a university magazine and is contractually controlled in its treatment of personal information) should not require consent.

Personal Information
Personal information means information about an identifiable individual. PIPEDA only regulates the treatment of personal information, but the definition is broad and only excludes information in aggregate form. If there is a reasonable chance that an individual can be identified from a piece of information, then that information qualifies as personal information.

Examples of "personal information" include identifying numbers, evaluative and opinion material, work records, financial information and records, personal opinions and all forms of personal health information.

Note that PIPEDA expressly exempts an individual's name, business title, and business address and telephone number from the definition of personal information.

Purpose Statement
A purpose statement must be made in order to obtain valid consent to collect, use, and disclose personal information in the course of commercial activity. A purpose statement must be broad enough to allow the desired use, but not so broad as to be meaningless.

Example of a Good Purpose Statement	Example of an Overly Broad Purpose Statement
We will use this information to offer you goods and services that we offer to our community of alumni and may make these offers by telephone or mail.	We will use this information to support our advancement activity.

Sensitivity
PIPEDA recognizes that some information is more sensitive than other information. For example, medical records and income records are more sensitive than a record that merely contains a home address and telephone number. The form of consent required by PIPEDA depends on the sensitivity of the information in question. Sensitivity should guide your answer to the following questions:

- Do we seek express consent or rely on implied consent?
- Do we allow people to "opt out" or, conversely, ask them to "opt in"?
- How specifically do we communicate our purpose?

PIPEDA Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization,

in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a check off box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.