# PRIVACY IN BRITISH COLUMBIA



**RESOURCES**

***Privacy Breaches- Tools and Resources April, 2012 OIPC***

---

Under the FIPPA, VIU must collect, use, and disclose personal information in a lawful and appropriate manner.

**Overview**

A classic definition of "privacy" is "the right to be left alone." Privacy encompasses the freedom from intrusions into one's physical space, and the right to control disclosure of one's private information. For VIU's purposes, however, "privacy" can best be defined as a set of rules governing the collection, use, disclosure, protection, storage and retention of personal information.

The privacy rules applicable to VIU are set out in the Freedom of Information and Protection of Privacy Act (FIPPA). The purpose of this information is to summarize the privacy-related requirements of the FIPPA at a high level for the benefit of VIU staff and faculty members. It is not intended to be a substitute for legal advice.

**Privacy Laws in B.C.**

VIU is subject to the FIPPA, which is one of several privacy laws that apply in British Columbia. Following are these laws and examples of organizations that are subject to them.

| | |
|---|---|
| Applicable Law: | *Freedom of Information and Protection of Privacy Act* (FIPPA) |
| Examples: | VIU, BC Ministry of Finance; ICBC; City of Nanaimo |
| Applicable Law: | *Personal Information Protection Act* (PIPA) |
| Examples: | CUPE, Tim Horton's |
| Applicable Law: | Federal *Privacy Act* |
| Examples: | Canada Revenue Agency; RCMP; Canada Post |
| Applicable Law: | *Personal Information Protection and Electronic Documents Act* (PIPEDA) |
| Examples: | Telus; Royal Bank; WestJet |

In addition to the above laws, BC also has a Privacy Act (which is not the same as the federal Privacy Act). The BC Privacy Act gives individuals the right to sue others, and receive damages, for willfully violating their privacy or using their name or portrait for the purpose of advertising property or services, without that person's consent.

**Overseeing compliance with the FIPPA**

In accordance with Section 6.6 of the FIPPA, the Board of Governors delegates the President and Vice-Chancellor of VIU as the head of the local public body. The President is ultimately responsible for VIU's implementation and adherence to the FIPPA but has delegated the day-to-day operational matters to the VIU University Secretary.

**Application of the FIPPA**

The FIPPA regulates the activities of the following individuals at VIU:

a. employees, including staff and faculty members;
b. volunteers; and,
c. employees, officers, directors, affiliates, and subcontractors of service providers (ie. persons or corporate entities retained under a contract to perform services for VIU).

The FIPPA does not regulate the activities of students, unless they are acting as employees, volunteers or service providers of VIU.

The FIPPA does not apply to independently incorporated entities that are associated with VIU, such as the Alumni Association.

**Privacy Rights**

Under the FIPPA, individuals have the right to expect public bodies to collect, use, disclose, retain and protect their personal information in a lawful and appropriate manner. They also have the right to:

- access their own personal information;
- request correction of their own personal information if they believe it is inaccurate;
- consent to the collection, use and disclosure of their own personal information; and
- complain to the Information and Privacy Commissioner if they believe their privacy has been breached.

Only private individuals have a right to privacy. Companies and other organizations do not have privacy rights.

Under some circumstances, an individual's privacy rights may be exercised by somebody else if he or she is under the age of 19, physically or mentally unfit, or deceased. For more information, refer to the section "Minors, Mentally Incapable and Deceased Individuals".

## Personal Information

"Personal information" comprises all recorded information about an identifiable individual, with the exception of the names and business contact information of employees, volunteers and service providers.

Personal information must have a precise, direct connection with one identifiable individual. For more information, refer to the information sheet "What is Personal Information?"

**Is an address Personal Information?**

- "123 Main Street" is **not** personal information (because it can't, by itself, be linked to an identifiable individual) .
- "Jane Doe works at 123 Main Street" is **not** Jane's personal information (because it is her business contact information).
- "Jane Doe lives at 123 Main Street" **is** Jane's personal information.

## Collecting Personal Information

The FIPPA lists several circumstances under which personal information may be collected. For example, section 26(c) of the FIPPA authorizes us to collect information if it "relates directly to and is necessary for an operating program or activity" of VIU.

Generally, personal information must be collected with the individual's knowledge. Covert collection of personal information is only permissible in exceptional circumstances, as defined in VIU Policy 44.17 and Procedure 44.17.001 *Audio Video Security Systems.*

Personal information must usually be collected directly from an individual. Indirect collection of personal information is only authorized under limited circumstances.

**Direct vs. Indirect Collection**

- If you ask John for his home address, you are directly collecting his personal information. This is the recommended method of collection.
- If you ask John's friend, Mary, for John's home address, you are indirectly collecting information about John. In most circumstances, this method of collection is not authorized.

## Using Personal Information

Generally, VIU is only authorized to use personal information for the purpose for which it was obtained or compiled or for a use consistent with that purpose. Therefore, it is essential for you to know the purpose for which VIU obtained the data.

**Consistent Use**

The VIU Library collects information from students for purposes related to library use. It would not be consistent to use this information for fundraising purposes.

Many IT systems provide the ability to store large amounts of personal information in centralized data repositories. When personal information collected for different purposes is mixed together in a single system, it becomes more likely that the purposes for collection will be forgotten and the data will be used inappropriately. Where possible, therefore, databases of personal information should only be linked when they were collected for a consistent purpose.

## Disclosing Personal Information

The FIPPA contains a long list of circumstances under which we are authorized to disclose personal information. The Office of the University Secretary has issued information sheets that explain some of the most

The Office of the University Secretary has issued information sheets that explain some of the most common circumstances, including: "Student and Alumni Privacy Issues"; "Employee Privacy Issues"; "Disclosing Personal Information to Law Enforcement Agencies and Government Bodies"; "Disclosing Personal Information in Emergencies" and "Disclosing Personal Information Outside Canada".

Personal information may be disclosed in two ways:

1. **Internal disclosure:** This is disclosure of personal information to other VIU employees, volunteers or service providers. As a rule, internal disclosure is permitted on a "need-to-know" basis.

2. **External disclosure:** This is disclosure of personal information to somebody outside VIU. External disclosure is tightly restricted and generally requires the written consent of the individual.

**Internal vs. External Disclosure**

- VIU staff may need to share students' financial information with each other for the purpose of processing student loan requests. This is **internal disclosure** within VIU and is permitted on a "need-to-know" basis.
- VIU staff may also receive questions about students' financial situations from the students' parents or legal representatives. This is **external disclosure,** which usually requires the student's written consent.

**Protecting Personal Information**

Under the FIPPA, we are required to protect personal information by "making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal". VIU requires individual units to ensure that the appropriate security measures are observed for records containing personal or other confidential information.

For an overview of requirements governing the security of personal information, refer to the information sheet "Security of Personal Information".

Many privacy protection issues arise out of the use of information technology because the ability to store large amounts of data on personal computers and other devices has significantly increased the risk of serious privacy breaches.

Outsourcing data storage and analysis to specialized service providers may also have a significant impact upon security and privacy. VIU remains ultimately responsible for the security of data we outsource, so we are obliged to ensure that our service providers have the appropriate safeguards in place to protect this data.

**Storing Personal Information Outside Canada**

Generally, VIU cannot allow personal information to be stored or accessed outside Canada without the written consent of the individual. This limits our ability to use "cloud computing" services or to outsource data storage or processing services outside Canada.

**Retaining Personal Information**

Retention periods must be established and followed for all records, including records containing personal information. All records must be retained for as long as they are required to meet legal, administrative, operational, and other requirements of the University.

The FIPPA requires VIU to retain personal information for a minimum of one year after it is used to make a decision that directly affects the individual. The purpose of this "privacy retention" requirement is to give the individual a reasonable opportunity to obtain access to his or her personal information. While the FIPPA does not impose a maximum retention period for personal information, it is considered good practice not to retain personal information longer than necessary. Therefore, the growing tendency to store data permanently (on the principle that it is cheaper to do so than to selectively delete data) is often inconsistent with good privacy practices.

**Privacy Retention**

VIU has just hired an employee. All the resumes and other personal information for all applicants for that position must be retained for at least one year.

**Ensuring Accuracy and Completeness of Personal Information**

An individual who believes there is an error or omission in his or her personal information may request the information to be corrected. If VIU does not make a correction, it must annotate the information with the correction that was requested but not made.

**Conducting Privacy Impact Assessments**

New systems, projects, programs and activities, and agreements with service providers may all have an impact upon privacy. The process used to evaluate these privacy implications is called a **Privacy Impact Assessment** (PIA). Under the FIPPA, VIU is obliged to conduct PIAs and, in some cases, is required to submit them to the Information and Privacy Commissioner for review and comment.

PIAs must be reviewed and approved by the University Secretary.

**Dealing with Privacy Breaches**

Privacy breaches occur when there is unauthorized access, collection, use, disclosure or disposal of personal information. Privacy breaches may cause significant harm to affected individuals and may also constitute an offence under the FIPPA.

You are required to notify the University Secretary if you have reason to believe that there has been a privacy breach.

Additional tools can be found on the Guidance Documents webpage of the Office of the Information and Privacy Commissioner (OIPC) website for public bodies.