



a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

A photograph of the UBC campus featuring the iconic clock tower, modern buildings, and lush greenery with colorful flowers in the foreground.

ACCESS and PRIVACY at UBC

A Guide for Faculty and Staff

ACCESS AND PRIVACY MANAGER

Direct Line: 604-822-2451

FREEDOM OF INFORMATION SPECIALIST

Direct Line: 604-822-2139

access.and.privacy@ubc.ca

OFFICE OF THE UNIVERSITY COUNSEL

Old Administration Building - 2nd Floor
6328 Memorial Road
Vancouver BC V6T 1Z2

Fax: 604-822-8731

<http://universitycounsel.ubc.ca/information-and-privacy/>



This guide summarizes the requirements of the *Freedom of Information and Protection of Privacy Act (FIPPA)*. The FIPPA applies to all UBC faculty members, staff, volunteers, and service providers.

The FIPPA has two purposes:

- **Freedom of Information:** to make public bodies more open and accountable by providing the public with a legislated right of access to government records, and
- **Protection of Privacy:** to protect personal privacy by prohibiting the unauthorized collection, use or disclosure of personal information by public bodies.

ACCESS TO INFORMATION

How does somebody request information from UBC?

Most requests received by UBC are for information that is not sensitive or confidential; these are called routine requests. Faculty and staff should make every reasonable effort to respond to routine requests following their units' established procedures or protocols they have set up with the Office of the University Counsel (OUC).

Requests for records that may contain sensitive or confidential information are called freedom of information (FOI) requests. These requests are processed by the OUC in accordance with procedures set out in the FIPPA.

How are FOI requests made?

FOI requests must be made in writing. Requesters may put the request in a letter, fax or email. UBC has 30 business days to respond from the date received, so UBC faculty and staff should forward all FOI requests to the OUC without delay.

What records can be requested?

The FIPPA applies to all records in the custody or under the control of UBC. "Records" include all recorded information in paper and electronic form. For example:

- emails, spreadsheets and other electronic documents
- letters, memos, reports, newsletters, draft documents
- calendars, agendas, minutes
- handwritten notes, journals, sticky notes
- photographs, videos and sound recordings

Do all requested records have to be released?

Not all information must be released in response to an FOI request. The OUC may redact (black out) information if it falls under any of the "exceptions to disclosure" listed in the FIPPA. For example, information may be withheld if its disclosure would:

- unreasonably invade a third party's privacy
- harm UBC's financial interests
- reveal advice or recommendations
- harm somebody's safety or the security of a facility or system

The following factors are not relevant in deciding whether to withhold information:

- the requester's identity
- the fact that the records may be used to embarrass UBC or any of its staff

Is there a cost for making an FOI request?

FOI requests may be subject to a copying fee as well as an hourly fee for the time spent locating and retrieving records (the first three hours is free of charge). UBC cannot, however, charge individuals a fee for access to their own personal information.

What if requesters are dissatisfied with UBC's response?

Requesters can ask the Information and Privacy Commissioner for British Columbia to review UBC's response to their access requests. The Commissioner's Office is independent of government and has the authority to issue binding orders to resolve disputes related to FOI requests.

PROTECTION OF PRIVACY

How does the FIPPA regulate privacy?

Under the FIPPA, UBC must collect, use and disclose personal information in a lawful and appropriate manner. The FIPPA also gives individuals the right to:

- access their own personal information
- ask for their own personal information to be corrected if they believe it is inaccurate
- consent to the disclosure of their own personal information
- complain to the Information and Privacy Commissioner about privacy breaches

What is personal information?

"Personal information" is defined as "recorded information about an identifiable individual", e.g. biographical, financial, educational and employment information. As an exception, the name and work contact information of an employee is NOT considered to be personal information.

How can UBC collect personal information?

Personal information should only be collected when it relates directly to and is necessary for a program or activity of UBC, and only from the individual, rather than from a third party. When we collect personal information, we should inform the person of

- the purpose for collecting the information
- the legal authority for collecting it
- the title and contact information of a UBC employee who can answer questions about the collection.

How can UBC use personal information?

We may only use personal information for the purpose it was obtained or compiled, or for a use consistent with that purpose.

How can personal information be shared?

We may disclose personal information to other UBC staff on a "need-to-know basis". Disclosure of personal information outside UBC is highly restricted and should only be done with the authorization of the OUC.

How can UBC protect personal information?

Under the FIPPA, we are required to make "reasonable security arrangements" to safeguard personal information in UBC's custody or under its control. Personal information stored in electronic format is especially vulnerable to loss or misuse. Wherever possible, it should be stored on secure servers rather than PCs or portable devices. If it is essential to store personal information on portable devices, it must be encrypted.

Personal information may not be stored or accessed outside Canada. This restricts UBC's use of "cloud computing" applications, e.g. Gmail and Facebook.

UBC service providers with access to personal information must sign contracts requiring them to protect the information.

For how long do we have to keep personal information?

Personal information must be retained for at least one year after it is used to make a decision that directly affects the individual. If the information has not been used to make a decision, this retention requirement does not apply.

Privacy Breaches

Unauthorized collection, use, disclosure or disposal of personal information is a serious matter and must be reported immediately to the OUC for investigation.

What is a Privacy Impact Assessment (PIA)?

This is an assessment tool designed to ensure compliance with the FIPPA's privacy requirements. UBC is required to perform a PIA for any new or substantially revised program, system, or other initiative that involves personal information.



Everyone at UBC has a role to play in ensuring compliance with the requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA). While the University Council has overall responsibility for administering the FIPPA, all faculty and staff have responsibilities relating to access and privacy.

WHAT ARE YOUR RESPONSIBILITIES?

Access to Information

- Be aware of the difference between routine requests and FOI requests.
- Forward new FOI requests to the OUC as soon as you receive them.
- Assist the OUC to locate and retrieve records in response to FOI requests.

Protection of Privacy

- Collect personal information with proper authority, using a privacy notification.
- Use personal information for the purpose it was collected.
- Share personal information within UBC on a need-to-know basis.
- Do not share personal information outside UBC without approval.

Records Creation and Retention

- Follow applicable records management and retention standards.
- Create records when necessary to fulfill operational requirements.
- Ensure that all your communications are professional.

Security

- Ensure personal information is securely stored and transmitted.
- Store personal information on secure servers wherever possible. If you must store personal information on mobile devices, it should be encrypted.
- Do not store personal information outside Canada without approval from the OUC.

WHAT IS THE ROLE OF THE UNIVERSITY COUNSEL?

The University Council has been delegated the authority and responsibility for ensuring that UBC complies with its access to information and privacy-related obligations.

Reporting to the University Council, the Access and Privacy Manager is responsible, with the assistance of the Freedom of Information Specialist, for:

- responding to FOI requests
- handling investigations and inquiries by BC's Office of the Information and Privacy Commissioner
- investigating complaints about alleged violations of privacy and requests for correction personal information
- reviewing Privacy Impact Assessments
- helping to develop and implement UBC policy, procedures, standards and guidelines on FIPPA compliance
- providing advice and training to faculty and staff on FIPPA-related matters

WHAT IS THE ROLE OF BC'S INFORMATION AND PRIVACY COMMISSIONER?

- Promotes and protects access and privacy rights
- Investigates and resolves complaints about public bodies' responses to freedom of information requests
- Investigates and resolves complaints about the collection, use, disclosure, retention and protection of personal information
- Provides advice and public education about access and privacy issues