University of Victoria

Protection of Privacy Policy

University Policy No: GV0235
Classification: Governance
Approving Authority: Board of Governors
Effective Date: XXX 2025
Supersedes: July 2018
Last Editorial Change: May 2025
Mandated Review: June 2028

Associated Procedures:
Procedures for Responding to a Privacy Incident or Privacy Breach
Procedures for the Management of University Surveillance Systems
Procedures for the Disclosure of Student Personal Information in Emergency or Compelling Circumstances
Procedures for the Management of Personal Information
University Information Security Classification Procedures
Procedures for Responding to the Loss or Theft of a Mobile Computing Device

PURPOSE

1.00 This policy articulates how the university complies with the privacy components of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

DEFINITIONS

2.00 For the purposes of this policy, the following definitions apply.

Administrative Authority means individuals with administrative responsibility for Units including but not limited to: Vice-Presidents, Associate Vice-Presidents, Deans, Chairs, Directors, Executive Directors, the Chief Information Officer, and other Unit Heads.

Consistent Purpose means a use or disclosure of Personal Information which is consistent with the purposes for which the information was obtained or compiled if the use or disclosure:

(a) has a reasonable and direct connection to that purpose, and
(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the Unit that uses or discloses the information or causes the information to be used or disclosed.

Contact Information means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email, or business fax number of the individual.

Data means digital or physical records, including personal information, held by the university.

Delegation Instrument means a document outlining the authority for an employee of the university to conduct activities and perform duties required under FIPPA required to be conducted by the head of the public body.

Disclose means to transmit, provide, or make available, intentionally or unintentionally, data by any means to a person.

Employee in relation to the university, and for the purposes of this Policy and it's associated procedures, each reference herein to Employee includes Officers of the university (E.g. members of Senate and the Board of Governors), faculty members, and volunteers.

Monitor/Monitored (verb) means a Surveillance System is used to view live footage of an area without creating a record of that observation.

Personal Information means recorded information about an identifiable individual other than Contact Information.

Privacy and Access to Information Office is the university department under the leadership of the Corporate Privacy Officer, responsible for ensuring compliance with FIPPA and this policy.

Privacy Breach refers to a confirmed case of unauthorized access to or collection, use, disclosure or disposition of Personal Information. Such activity is considered to be 'unauthorized' if it occurs in contravention of the Freedom of Information and Protection of Privacy Act, or the University's Protection of Privacy Policy (GV0235).

Privacy Impact Assessment (PIA) means a legally required assessment that the university conducts to determine if a current or proposed system, project, program, or activity meets or will meet the requirements of FIPPA, this policy, and its associated procedures.

Privacy Incident means an unconfirmed but potential Privacy Breach.

Record (*noun*) includes books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other thing on which information is recorded or stored by

graphic, electronic, mechanical, or other means, but does not include a computer program or any other mechanism that produces records.

Record/Recorded (*verb*) means a Surveillance System is used to convert images and/or sound into a record that can be reproduced.

Service Provider means a third party individual, organization, company, application, contractor, service, or software as service retained under contract to provider services or deliver work on behalf of the university.

Surveillance System means an authorized video recording system (with or without audio) or audio recording system used by the university to monitor or record people or area. For the purposes of this policy and its associated procedures, surveillance does not include the use of personal video equipment or the recording or broadcasting of public events, educational activities, or recordings by UVic Audiovisual and Multimedia Services.

Unauthorized Disclosure means the disclosure, production, or provision of access to Personal Information which is not authorized by the *Freedom of Information and Protection of Privacy Act* or another applicable statute.

Unit means academic or administrative areas at the university, including but not limited to:

- faculties,
- departments,
- divisions,
- offices,
- schools, and
- centres.

Use of Personal Information means the employing or handling Personal Information by an Employee to accomplish the university's objectives, for example, to:

- administer a program or activity;
- provide a service; or
- determine someone's eligibility for a benefit or suitability for a job.

JURISDICTION/SCOPE

3.00 This policy applies to all Employees and Units. It applies to all Personal Information in the custody or under the control of the university.

POLICY

4.00 The university will manage all Personal Information in accordance with FIPPA, the *University Act*, as well as all applicable university policies and associated procedures, collective agreements, and contracts.

Accountability for Personal Information

5.00 The President will designate a senior administrator to act as head under FIPPA who will be responsible for the administration of FIPPA and this policy. The General Counsel is designated by the President as the head of the university for the purposes of FIPPA.

General Counsel

6.00 As the head, the General Counsel is responsible for the overall co-ordination of privacy and access functions.

6.01 The General Counsel will carry out their duties in collaboration with the University Secretary and the University Archivist, who are responsible for the maintenance of the university's Records management program.

6.02 The General Counsel may delegate their authority under FIPPA, as necessary to accomplish their duties under FIPPA. The Corporate Privacy Officer carries the delegated authority of the General Counsel to lead the Privacy and Access to Information Office, in accordance with the terms and conditions as enumerated in the delegation instrument.

Corporate Privacy Officer

7.00 In collaboration with the University Secretary, the University Archivist, and the Chief Information Officer, the Corporate Privacy Officer is responsible for promoting, monitoring, and reporting on compliance with FIPPA as it relates to university privacy, records management, and information security policies. Under this policy, the Corporate Privacy Officer's responsibilities include:

- leading the Privacy and Access to Information Office;
- providing advice on privacy matters;
- providing privacy training;
- providing ongoing assessment of privacy risks for the university;
- providing guidance and review of Privacy Impact Assessments under s. 27.00;
- responding to privacy incidents and complaints;
- investigating concerns about privacy issues; and
- working with partners across campus towards reconciliation related to data initiatives involving Indigenous communities.

8.00 Where the Privacy and Access to Information Office establishes that there is a significant privacy risk, in accordance with the university's policies and procedures for managing data risk, the Corporate Privacy Officer may investigate

and/or recommend to the appropriate Administrative Authority corrective action, suspension, or termination of a project or activities.

9.00 The Administrative Authority must carefully consider the results of an investigation and/or recommended action by the Corporate Privacy Officer when making a decision, in accordance with policies and procedures on data risk and signing authorities.

Administrators

10.00 An Administrative Authority or manager is responsible for:

- familiarizing themselves with the requirements in FIPPA, this policy, and its associated procedures;
- discussing with the Privacy and Access to Information Office all privacy concerns as they arise;
- communicating these requirements to the Employees in their Units;
- ensuring that the management of Personal Information in the custody or under the control of their Units meets the requirements of FIPPA, this policy, and its associated procedures;
- ensuring that all Employees in their Units complete the annual privacy training; and
- reporting to the Privacy and Access to Information Office any privacy incidents or breaches of FIPPA, this policy, or its associated procedures in accordance with the university's Procedures for Responding to a Privacy Incident or Breach.

Employees

11.00 An Employee with access to Personal Information as a part of their duties are responsible for:

- treating all Personal Information they access in accordance with FIPPA and this policy;
- familiarizing themselves and complying with the requirements in FIPPA, this policy, and its associated procedures;
- completing the annual privacy training;
- consulting as necessary with the appropriate authority regarding the requirements in FIPPA, this policy, and its associated procedures; and
- reporting to their Administrative Authority or manager or Access to Information and Privacy Office any privacy incidents or breaches of FIPPA, this policy, or its associated procedures in accordance with the university's Procedures for Responding to a Privacy Incident or Breach.

Service Providers

12.00 The university will require a service provider whose work on behalf of the university involves the collection, use, or disclosure of Personal Information to abide by this policy and FIPPA in its handling of Personal Information on behalf of the university, and may require the service provider to sign a confidentiality agreement or have a Data Protection Schedule attached to a contract.

12.01 Any proposed work to be conducted by a service provider must be reviewed by a privacy impact assessment prior to conducting work

Collection Notice

13.00 The university is required to collect certain Personal Information from individuals to fulfill its mandate under the *University Act*. All other Personal Information collected by the university will be authorized by FIPPA, the *University Act*, or other applicable legislation.

14.00 Unless authorized by FIPPA, another enactment, or an individual, the university will provide notice before collecting Personal Information directly from an individual.

15.00 If notice is required, the university will make the following information available to an individual from whom Personal Information is being collected:

(a) the purpose for which the Personal Information is being collected;
(b) the legal authority to collect the Personal Information; and
(c) the Contact Information of someone who can provide details about the collection.

16.00 If an Employee or Administrative Authority is unsure whether notice is required before collecting information, contact the Privacy and Access to Information Office.

Use, Disclosure, and Retention of Personal Information

17.00 An Employee must only use and disclose the Personal Information in the university's custody or control:

(a) for a purpose consistent with the reason the information was collected;;
(b) in a manner to which an individual has consented;
(c) as permitted or required by FIPPA or as authorized or required by other law;
(d) for research and statistical purposes; or
(e) for archival or historical purposes.

18.00 An Employee must only use, and disclose Personal Information that is necessary for the performance of their duties. An Employee may permit others in their Unit or other university Unit's to access Personal Information if the purpose is consistent with the purpose for which the information was obtained.

18.01 An Employee must consult their Administrative Authority, manager, or the Privacy and Access Office if they are uncertain whether a purpose is consistent with the purpose the Personal Information was collected.

19.00 The university may disclose Personal Information to students and individuals or organizations outside the university as permitted by FIPPA, as authorized or required by an enactment, as permitted by this policy, or its associated procedures.

19.01 Personal Information shall only be disclosed in compliance with the Procedures for the Management of Personal Information.

19.02 Disclosure of the Personal Information without consent is permitted in certain circumstances as required by FIPPA, other legislation, or the advice of the Privacy and Access to Information Office.

19.03 If an Employee is in doubt whether to disclose Personal Information, the Employee will consult with their Administrative Authority, manager, or the Privacy and Access to Information Office.

20.00 Disclosing Personal Information outside Canada must be done in compliance with FIPPA and the Procedures for the Management of Personal Information.

Retention

21.00 The university will retain Personal Information collected from individuals in accordance with FIPPA and the university-wide records classification, retention and disposition plan.

22.00 An Administrative Authority or manager is responsible for understanding the Directory of Records and the appropriate retention and disposition schedules as defined by the Records Management Policy.

22.01 The university will retain all Personal Information used to make a decision about an individual that does not have a retention and disposition schedule for one year.

Ensuring Accuracy of Personal Information

23.00 The university will make every reasonable effort to ensure that the Personal Information in its custody or under its control is accurate and complete and will allow an individual to confirm the accuracy of their personal information.

23.01 Procedures for the Correction of Personal Information are contained within the university's Procedures for the Access to and Correction of Information.

Safeguards for Personal Information

24.00 The university will protect Personal Information in its custody or control by making reasonable security arrangements against risks of unauthorized access, collection, use, disclosure, or disposition.

Individual Access to Personal Information

25.00 Individuals have a right to access Personal Information about themselves, subject to exceptions under FIPPA. Access to Personal Information is provided in accordance with the university's Access to and Correction of Information procedure.

26.00 Individuals have a right to request corrections to Personal Information about themselves, subject to exceptions under FIPPA. Corrections to Personal Information are provided in accordance with the university's Access to and Correction of Information procedure.

Privacy Impact Assessments

27.00 The Administrative Authority must ensure a Privacy Impact Assessment has been completed for all new systems, projects, programs, or activities and substantially modified systems or activities. The nature and extent of the assessment will be based upon the risks assessed, in accordance with policies and procedures regarding data risk.

27.01 Before committing the university to a project, program, system, initiative, or activity or before procurement, the Administrative Authority must direct an Employee from their Unit who has appropriate technical knowledge to draft, with guidance from the Privacy and Access to Information Office, a PIA.

28.0 The Privacy and Access Office is the office of primary responsibility for the storage and disposal of Privacy Impact Assessments.

Surveillance Systems

29.0 The university may use Surveillance Systems to:

(a) improve personal safety on university property by acting as a deterrent where other practical options have failed or increasing the likelihood of identifying individuals who may have commit criminal activity;
(b) assist with, upon the request of law enforcement agencies, the investigation of any suspected criminal activity;
(c) assist with the protection of university assets and infrastructure; or
(d) aiding in the investigation of violations of the university's Sexual Violence Prevention and Response Policy (GV0245).

29.01 Surveillance Systems shall not be used to monitor or record areas where the university community or public have a reasonable expectation of privacy.

29.02 The university will deploy Surveillance Systems only as an exceptional step to address problems or risks identified in section 29, where a less privacy-invasive alternative is not practical. Surveillance Systems will be designed to minimize the impact on privacy. The privacy impact of the proposed Surveillance System will be assessed and documented in a PIA.

29.03 Approval is required prior to installation of a Surveillance System. The General Counsel is responsible for approval of the installation, following input from the Vice-President Finance and Operations and Corporate Privacy Officer, and confirmation that the installation is necessary to address real, pressing, and substantial problems or risks and that a less privacy-invasive alternative is not practical.

29.04 Surveillance Systems shall be operated on a day-to-day basis and administered by the university's Campus Security department.

30.0 In accordance with the Procedures for the Management of University Surveillance Systems, the university will provide notice of the use of Surveillance Systems by prominently displaying signage at the perimeter or entrance to the area being monitored or recorded to notify individuals that such systems are or may be in use before they enter any area under surveillance.

31.0 Sections 29.0 and 30.0 apply only to Surveillance Systems installed with notice, i.e., overt surveillance.

Challenging Compliance with the Privacy Policy

32.0 An Individual is entitled to challenge the university's compliance with this policy.

32.01 An Employee who receives a complaint or inquiry about compliance with the policy should attempt to resolve the issue with the assistance of a supervisor.

32.02 An Individual may make a formal complaint or inquiry about compliance with this policy by contacting the Privacy and Access Office.

Compliance with Procedures

33.0 Employees (including faculty) must comply with the following procedures associated with this policy:
33.01 Procedures for Responding to a Privacy Incident or Privacy Breach
33.02 Procedures for the Management of University Surveillance Systems
33.03 Procedures for the Disclosure of Student Personal Information in Emergency or Compelling Circumstances
33.04 Procedures for the Management of Personal Information

AUTHORITIES AND OFFICERS

I. Approving Authority: Board of Governors
II. Designated Executive Officer: President
III. Procedural Authority: President
IV. Procedural Officer: General Counsel

RELEVANT LEGISLATION

University Act
Freedom of Information and Protection of Privacy Act

RELATED POLICIES AND DOCUMENTS

Associated Procedures

- Procedures for Responding to a Privacy Incident or Privacy Breach
- Procedures for the Management of University Surveillance Systems
- Procedures for the Disclosure of Student Personal Information in Emergency or Compelling Circumstances
- Procedures for the Management of Personal Information
- University Information Security Classification Procedures
- Procedures for Responding to the Loss or Theft of a Mobile Computing Device

Records Management Policy (IM7700)

- Procedures for the Access to and Correction of Information

- Procedures for the Management of University Records
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Information Security Policy (IM7800)

- Procedures for Responding to an Information Security Incident

Directory of Records

EXTERNAL RESOURCES

Canadian Standards Association Privacy Code