

Original Approval Date: February 1, 2007  
 Most Recent Approval Date: December 5, 2014  
 Most Recent Editorial Date: May 13, 2015

Parent Policy: [Access to Information and Protection of Privacy Policy](#)

## Access to Information and Protection of Privacy Procedure

<b>Office of Administrative Responsibility:</b>	Information and Privacy Office
<b>Approver:</b>	Provost & Vice-President (Academic)
<b>Scope:</b>	Compliance with this University procedure extends to all members of the University community.

### Overview

As a public post-secondary institution, the University of Alberta has a responsibility to protect the public interest and has a commitment to the highest standards of institutional integrity, transparency and accountability.

The University of Alberta is governed by the Alberta *Freedom of Information and Protection of Privacy Act and Regulations (the Act)* and other provincial and federal privacy legislation.

### Purpose

To ensure consistent actions by members of the University community with regard to the collection, use, disclosure, protection and disposition of information under the **custody** or **control** of the University that is gathered or generated in the course of operating the programs and all other activities of the University and with regard to responding to requests for information.

## **PROCEDURE**

### 1) ACCESS TO INFORMATION

Access to recorded information under the custody or control of the University will be provided by three methods:

- a) Active dissemination of information – information routinely available to the public.

All **Units** of the University:

- i) May publish information for the public in many formats such as printed reports, calendars, brochures, and through University web-sites. (Some charges may apply.)
- ii) Will make available to the public, in a manner whereby the public may inspect such material, any manual, handbook or other guideline used by employees in decision-making processes that affect the public in administering or operating the programs or activities of the University.

- b) Routine disclosures of information - information available without a formal request.

All Units of the University will:

- i) Provide access to information in the custody or control of the unit in accordance with University approved policies and procedures.
- ii) Disclose information as required by:
  - (1) the Post-Secondary Learning Act, and,
  - (2) other enactments of Alberta or Canada in accordance with legislative paramountcy, and,
  - (3) program and administrative needs in accordance with the purpose for which the information was collected or compiled or for a use consistent with that purpose.

- iii) In accordance with approved University records classification plans, records retention and disposition schedules and archival systems, specify categories of records that are available to the public through routine disclosure without a formal request under the Act (e.g. reports, publications, policies and operational manuals).
  - iv) Dispose of information either by transfer to the University Archives or by destruction in accordance with the approved records retention schedules and disposal schedules.
- c) Disclosures in response to a formal request for information under the Act.
- i) The University will process formal requests for records not available through active dissemination or routine disclosure under the provisions of the Act.
  - ii) All Units of the University that receive formal requests for information will process such requests through the **Information and Privacy Office (IPO)** in accordance with the requirements of the Act.
  - iii) Disclosure of information in support of research or a planning study/survey must be in compliance with the Access to Personal Information for Research/Studies Procedure.

## 2) MAKING A FORMAL REQUEST FOR INFORMATION

Individuals requesting information that is not actively disseminated or routinely available may make a formal request for access to information as follows:

- a) A request for access to information may be submitted to any office of the University of Alberta having custody of the responsive records.
- b) All formal requests for information shall be forwarded to the Information and Privacy Office which will act in the official capacity in responding to the request.
- c) The receiving office and the Information and Privacy Office shall assist the applicant in defining the information being requested and the time frame for the respondent records.
- d) The Information and Privacy Office will assist the applicant by clarifying the request, coordinating the search for responsive records, and if appropriate, providing a fee estimate and providing access to the records to the applicant in accordance with the Act.

## 3) RECORDS RETENTION AND DISPOSITION SCHEDULES

Each Unit of the University will attend to the following matters:

Adhere to approved records retention and disposition schedules for University records pursuant to the Records Management Policy and associated procedures. The University's Records Officer can provide guidance on these schedules.

## 4) MANAGEMENT AND PROTECTION OF PERSONAL INFORMATION

**Personal information** under the custody or control of the University will be managed by all Units of the University in a manner that protects the privacy of individuals.

To the extent that the matters are within their control, all University Units and employees will attend to the following matters in respect of personal information. These obligations apply to personal information handled by the University Unit in the course of its operations, or to which the employee has access in the course of his or her employment:

- a) Manner of Collection
  - i) Collect personal information as provided for under Part 2 of the Act, which states that:
    - (1) The University must only collect the personal information that is necessary for the University's operating program or activity; and
    - (2) Personal information should be collected directly from the individual the information is about, unless otherwise authorized under the Act.
  - ii) Ensure that **Notification Statements** are included on all collection documents, in the form found on the website of the Information and Privacy Office, or in a form that is otherwise approved by the Information and Privacy Office.

b) Accuracy and retention

Take all reasonable steps to ensure the accuracy of all personal information and retain such information in compliance with the Act. The Act states that if an individual's personal information will be used by the University to make a decision that directly affects the individual, the University must generally retain that personal information for at least one year.

c) Use of personal information

- i) Use personal information only for the purposes for which it was collected or other consistent purposes, or in accordance with the specifications of the Act. University employees will only access and use personal information as it is needed in order to fulfill their employment obligations.
- ii) Obtain **Informed Consent** as defined in the Act to use the personal information for other purposes.

d) Disclosure

Disclose personal information only as follows:

- i) for the purposes for which it was collected or compiled, or for a use consistent with that purpose; or
- ii) if Informed Consent to disclose the personal information for other purposes has been obtained from the individual; or
- iii) if the disclosure is otherwise authorized under Part 2 of the Act.

An Informed Consent form is available on the Information and Privacy Office's website.

Otherwise, personal information accessed in the course of operating the programs and all other activities of the University will be kept confidential.

e) Security

- i) Ensure the safe and secure storage and handling of all personal information against unauthorized access, use, disclosure and destruction in accordance with University Policies and Procedures and the Act. One key safeguard is the encryption of any mobile device that is used to store personal information, in accordance with the Encryption Procedure. Faculties, departments and administrative units may develop requirements that are appropriate for their area in order to ensure the safe and secure storage and handling of personal information.
- ii) Conduct a Privacy Impact Assessment where necessary, in accordance with guidance provided by the IPO, before implementing a major project that involves the collection, use or disclosure of personal information.

f) Disposal

Ensure the safe and secure disposal of all personal information in accordance with approved records retention schedules and disposition schedules. Records containing sensitive, personal or confidential information must be securely destroyed or deleted in accordance with the Information Technology Security Policy.

Any paper records containing personal information must be shredded with a cross shredder or placed in a secure shredding bin.

Any electronic devices containing personal information (for example a laptop, tablet, or smart phone) must be securely wiped. For University owned electronics, please contact SMS Surplus Services. A link to their website is provided below. For personally owned electronics, please contact Information Services & Technology (IST) or your local IT group for assistance.

g) Privacy and Security Acknowledgement

When requested, each employee who has access to Personal Information in the course of his or her work will acknowledge on an annual basis that they have read and understood this Procedure, and any other policies or procedures relevant to the privacy and security of Personal Information.

h) Training

Each employee who has access to Personal Information in the course of his or her work will take appropriate privacy and security training, which is identified by the IPO and/or the Information Technology Security Officer.

5) NON-COMPLIANCE

Non-compliance with this Procedure constitutes misconduct and may be handled under the applicable collective agreement, University policy, or law.

## **DEFINITIONS**

Definitions should be listed in the sequence they occur in the document (i.e. not alphabetical).

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use. [\[▲Top\]](#)

<b>The Act</b>	The <i>Freedom of Information and Protection of Privacy Act</i> , RSA 2000, Chapter F-25 and associated regulations, as amended from time to time.
<b>Custody</b>	Having <i>custody</i> of a record generally means having physical possession of a record that is related to the University's operation and administration.
<b>Control</b>	Having <i>control</i> of a record means having the power or authority to manage, restrict, regulate or administer the use or disclosure of the record.
<b>Unit(s)</b>	Administrative and/or organizational entities including faculties, departments, centres, institutes, administrative units and non-departmental units.
<b>Information and Privacy Office (IPO)</b>	The office of the University charged with the responsibility for ensuring the compliance of the University with the <i>Act</i> with delegated authority from the Head under the <i>Act</i> .
<b>Personal Information</b>	<p>Personal information means recorded information about an identifiable individual. This includes information such as the individual's:</p> <ol style="list-style-type: none"> <li>a. name and contact information, age, and gender</li> <li>b. student or employee ID #, or other identifying number</li> <li>c. application for employment, salary, employment evaluations, and other employment history</li> <li>d. grades, assignments, and other educational history</li> <li>e. health information or financial information</li> <li>f. race, national or ethnic origin, or colour</li> <li>g. religious or political beliefs or associations</li> <li>h. marital status or family status,</li> <li>i. biometric information, and</li> <li>j. criminal history.</li> </ol> <p>These are examples only, and not a comprehensive list. Further examples of personal information are set out in the Appendix to this Procedure, and in the <i>Act</i>.</p>
<b>Notification Statement</b>	A statement that informs the individual as to the purpose for which the information is collected; the legal authority for the collection; and, the contact information of an employee that can answer questions about the collection.
<b>Informed Consent</b>	Consent given freely in a prescribed manner and with full knowledge of the personal information to be provided and the use to be made of such information.

**Privacy Impact Assessment**

A privacy impact assessment is a due diligence exercise in which the organization, in collaboration with the Information and Privacy Office and the Information Technology Security Office, identifies and addresses potential privacy risks that may occur in the course of its operations. The form and length of a privacy impact assessment can vary, depending on the project.

**FORMS**

Should a link fail, please contact [uappol@ualberta.ca](mailto:uappol@ualberta.ca). [[▲Top](#)]

[Request to Access Information Form](#)

[Informed Consent for Disclosure of Personal Information](#)

[Example of FOIPP Notification Statement](#)

**RELATED LINKS**

Should a link fail, please contact [uappol@ualberta.ca](mailto:uappol@ualberta.ca). [[▲Top](#)]

[Information and Privacy Office](#) (University of Alberta)

[Privacy Highlights and Quick Tips](#) (University of Alberta)

[Encryption Procedure](#) (University of Alberta)

[Records Management Policy](#) (University of Alberta)

[Information Technology Use and Management Policy](#) (University of Alberta)

[Mobile Computing Security](#) (University of Alberta)

[Information Technology Security Policy](#) (University of Alberta)

[Supply Management Services – Surplus Service](#) (University of Alberta)

[Freedom of Information and Protection of Privacy Act](#) (Government of Alberta)

[Freedom of Information and Protection of Privacy Regulation](#) (Government of Alberta)