POLICY TEMPLATE

POLICY ON ACCESS TO INFORMATION AND PROTECTION OF PRIVACY (DRAFT)

Category: Leave this blank; a category will be assigned
Approval: The University Secretary, on the advice of the Policy Advisory Subcommittee, will identify the appropriate approval body(ies), e.g. Board of Trustees, Senate, VPOC, other
Responsibility: University Secretariat and Legal Counsel
Date: Date initially approved: Date of last revision:

Definitions:

Agent: means a person, with the authorization of the university, acting for or on behalf of the university for the purposes of the university and not the agent's own purposes, whether or not the agent has the authority to bind the university, whether or not the agent is employed by the university and whether or not the agent is being remunerated. For the purposes of this policy, a consultant is considered to be an agent.

Business Identity Information: information, including the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity. Business identity information is not considered to be personal information.

Data Classification Scheme: the university’s schema for classifying data and information to ensure the level of information protection and privacy is commensurate with the sensitivity and value of that data.

Directory of Records (DoR): means a list of the general classes or types of records prepared by or in the custody or control of the university.


Information Steward: the university officer or employee (faculty or staff) having primary responsibility for a record or group of records.

Non-University Records: records created or received as a result of personal activities and usually including such items as research and study notes, teaching materials, publications and personal communications of individual faculty, staff and students. Non-university records include
• records placed in the University Archives by or on behalf of a person or organization other than the university;

• a record respecting or associated with research conducted or proposed by an employee of the university or by a person associated with the university, subject to exceptions pursuant to FIPPA; and

• a record of teaching materials collected, prepared or maintained by an employee or by a person associated with the university for use at the university, subject to exceptions pursuant to FIPPA.

**Personal Health Information (PHI):** identifying information about an individual, in oral or recorded form, if that information relates to the physical or mental health of the individual and relates to the provision of healthcare to the individual, or includes the individual’s health card number.

**Personal Information (PI):** recorded information about an identifiable individual. See Schedule A for the full FIPPA definition.

**Personal Information Bank (PIB):** means a collection of personal information that is organized and capable of being retrieved using an individual’s name or an identifying number or particular assigned to the individual.

**Record:** as defined in FIPPA, any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,

• correspondence (including email), a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and

• subject to the regulations, any record that is capable of being produced from a machine readable record by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution

**Privacy Impact Assessment (PIA):** means an organizational risk management tool used to identify the effects of a given process or other activity on an individual’s privacy.

**Service Provider:** any third-party entity that provides services to the university, whether for compensation or for free.

**University Records:** records, in any media or format, within the university’s custody or under its control that are created or received, and maintained as evidence or information in the administration and operation of the activities of the university.

**Purpose/Reason for Policy:**

The purpose of this policy is to:
• set out the responsibilities of the university community regarding the right of access to records and information and the protection of privacy of personal information in accordance with the Freedom of Information and Protection of Privacy Act ("FIPPA"); and

• ensure that personal information in the university’s custody or control, including personal information that has been transferred to an agent or service provider, is handled and protected appropriately.

**Scope of this Policy:**

This policy applies to all university employees (including faculty, staff, and students employed by Queen’s), as well as members of the Board of Trustees, volunteers, service providers and agents, and any other individuals who collect, use, disclose, or otherwise handle records and information under the custody or in the control of Queen’s University.

This policy applies to all university records in all media and formats, including but not limited to paper, electronic documents and files, email, photographs, film, audio and video, and drawings.

This policy does not apply to non-university records.

This policy does not apply to records collected, prepared, maintained or used by or on behalf of the university in relation to any of the following, subject to exceptions pursuant to FIPPA:

- proceedings or anticipated proceedings before a court, tribunal or other entity relating to labour relations or to the employment of a person by the university;
- negotiations or anticipated negotiations relating to labour relations or to the employment of a person by the university between the university and a person, bargaining agent or party to a proceeding or an anticipated proceeding; or
- meetings, consultations, discussions or communications about labour relations or employment-related matters in which the university has an interest.

For records of personal health information, see the policy on the Handling of Personal Health Information.

**Policy Statement:**

Queen’s University affirms the importance of conducting its operations in ways that are open to public scrutiny. Queen’s University is also committed to the protection of privacy and personal information of individuals who work and study at the university, or who participate in the university community. Accordingly, the university will collect, use, disclose, retain, dispose of and protect records and information in accordance with FIPPA.

1. **Basic Principles**

   1.1 As a general rule, information contained in university records will be available to members of the university community and to the public subject to specific and limited exemptions. To
facilitate access, the university will describe university records in its directory of records and, where appropriate, in its index of personal information banks.

1.2 The collection, use, disclosure, retention and disposal of personal information contained in university records will be regulated so as to protect the privacy of individuals who are the subject of that information.

1.3 Consistent with its commitment to accountability and transparency, the university actively disseminates information about its operations, activities, policies, practices and procedures by regularly making public a wide range of information through, for example, its website and its official publications.

2. Access to Information

2.1 Access Right

i. Access will be granted to records and information in the university’s custody or under its control unless, upon reasonable grounds, the request for access is frivolous or vexatious, or is exempt, in accordance with FIPPA.

ii. Individuals will be granted access to their own personal information except where, in accordance with FIPPA, the disclosure:

- could reasonably be expected to interfere with a law enforcement matter;
- could reasonably be expected to reveal information received in confidence from another government body or its agencies;
- could reveal a trade secret or scientific, technical, commercial, financial, or labour relations information belonging to a third party;
- contains information related to tests or testing procedures used in the evaluation of students;
- is subject to solicitor-client privilege; or
- belongs to any other exemption or exclusion set out in FIPPA.

iii. The right of access may be subject to the payment of a fee required by university policy or practice for informal access requests, and under FIPPA for formal access requests.

2.2 Correction Right

i. Every individual who is given access to their own personal information has the right to request correction of the personal information where the individual believes there is an error or omission.

ii. A statement of disagreement will be attached to the personal information reflecting any correction that was requested but not made.
3. Protection of Privacy

3.1 Collection of Personal Information

i. Personal information will not be collected unless it is expressly authorized by statute, used for purposes of law enforcement, or necessary to the proper administration of a lawfully authorized activity.

ii. Personal information will be collected according to the following principles:
   - the personal information collected must be necessary to fulfill a legitimate university activity or purpose;
   - the personal information collected must be the minimum amount necessary for the activity or purpose; and
   - the personal information must be collected directly from the individual or if indirectly, with the clear knowledge and authority of the individual, or as permitted by FIPPA.

iii. When personal information is collected, notice will be provided to the individual of the following:
   - the legal authority for the collection;
   - the purpose for the collection and how the information is intended to be used; and
   - contact information for a university employee who can answer inquiries about the collection.

3.2 Use of Personal Information

i. Personal information will be used only:
   - for the purpose for which that information was obtained, compiled, or disclosed, or
   - for a use consistent with that purpose, or
   - with the consent of the individual.

ii. Personal information in alumni records may be used for the purpose of the university’s own fundraising activities in compliance with the requirements of FIPPA.

3.3 Disclosure of Personal Information

i. Personal information will be disclosed only to the person to whom the information relates except:
• where the individual has given consent, or

• for the purpose for which it was obtained, or

• where the disclosure is made to university employees, or to consultants or agents engaged by the university, where the disclosure of the information is necessary and proper for the performance of their duties.

ii. Personal information may be disclosed in compelling circumstances affecting the health and/or safety of an individual or individuals.

iii. Personal information may be disclosed on compassionate grounds to facilitate contact with a family member of an individual who is injured, ill, or deceased.

iv. Personal information may be disclosed to an institution or a law enforcement agency in Canada to assist with investigations.

v. Personal information in alumni records may be disclosed for the purpose of the university's own fundraising activities in compliance with the requirements of FIPPA.

vi. Personal information may be disclosed in compliance with any other exceptions cited in FIPPA.

3.4 Safeguarding Personal Information

i. Personal information in all formats (electronic, paper, verbal, or other) will be safeguarded throughout its lifecycle (collection, use, disclosure, processing, distribution, transfer, storage and disposal) through reasonable measures of protection.

ii. The measures of protection will include physical, administrative and technical controls as determined by the university’s information security policies, procedures and standards, and/or by external regulatory agencies.

iii. The nature of the measures of protection will vary depending on the classification and categorization of the information in accordance with the university’s data classification scheme.

iv. Contractual or other measures will be used to protect personal information that has been transferred to, or is collected by, agents and service providers.

v. If personal information is lost, stolen, or used or disclosed without authority, the responsible department or unit head will report the breach to the Chief Privacy Officer as soon as possible.

4. Records Retention and Disposal

4.1 An individual's personal information will be retained for at least one year after use. Thereafter the personal information will be disposed of in accordance with the university’s authorized records retention schedules.
4.2 Care will be taken in the disposal or destruction of personal information to prevent unauthorized access to the information.

When records are destroyed or deleted, all reasonable steps will be taken to ensure the information cannot be retrieved.

**Responsibilities:**

The **Principal and Vice-Chancellor** is the Executive Head of the university and has the authority and responsibility for decision-making under FIPPA.

The **Office of the University Secretariat and Legal Counsel** has operational responsibility for this policy and appoints a Chief Privacy Officer for the purposes of implementation.

The Chief Privacy Officer will:

- ensure the university responds to formal access to information requests in a timely fashion;
- develop procedures and guidelines and other user-friendly tools to support implementation by university departments and units;
- provide training and advisory services to employees of university departments and units so that the policy and procedures are understood and applied;
- maintain a network of contacts across university departments and units for the purpose of information-sharing, feedback, and continuous program improvement; and
- require the appropriate department or unit to conduct a privacy impact assessment where, in the opinion of the Chief Privacy Officer, the collection and/or use of records containing personal information poses a potential risk to the protection of privacy.

All Information Stewards will:

- take reasonable measures to ensure that records containing personal information are protected from unauthorized access or modification, and inappropriate use or disclosure, whether intentional or unintentional;
- report privacy breaches to the Chief Privacy Officer as soon as possible; and
- conduct a privacy impact assessment as directed by the Chief Privacy Officer.

All Department and Unit Heads will:

- report privacy breaches to the Chief Privacy Officer as soon as possible;
- conduct a privacy impact assessment as directed by the Chief Privacy Officer;
• ensure employees in their department or unit are aware of this policy and are appropriately trained; and

• ensure all other individuals to whom the policy applies who are engaged by, or work with, their department or unit are aware of this policy and are appropriately trained.

All university employees (including faculty, staff, and students employed by Queen’s), as well as members of the Board of Trustees, volunteers, service providers and agents, and individuals who collect, use, disclose, or otherwise handle records and information under the custody or in the control of Queen’s University will:

• ensure that general and personal information is handled according to this policy and in compliance with the Queen’s University data classification scheme;

• consult, as needed, the Chief Privacy Officer about the disclosure of confidential and personal information;

• cooperate with the Chief Privacy Officer, when required, in fulfilling formal requests for access to information;

• comply with this policy and any procedures issued in accordance with it.

<table>
<thead>
<tr>
<th>Contact Officer</th>
<th>Chief Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date for Next Review</td>
<td>2022/02/01</td>
</tr>
<tr>
<td><strong>Related Policies, Procedures and Guidelines</strong></td>
<td><strong>Records Management Policy</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Policy on the Handling of Personal Health Information</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Electronic Information Security Framework</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Policies Superseded by This Policy</strong></th>
</tr>
</thead>
</table>
**Schedule A: Personal Information**

As defined in the *Freedom of Information and Protection of Privacy Act* (RSO 1990, c.F31),

“Personal Information” means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual’s name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.