

<b>Policy Name:</b>	Access to Information and Privacy
<b>Originating/Responsible Department:</b>	Office of the General Counsel
<b>Approval Authority:</b>	Senior Management Committee
<b>Date of Original Policy:</b>	September 2019
<b>Last Updated:</b>	N/A
<b>Mandatory Revision Date:</b>	September 2024
<b>Contact:</b>	Manager, Privacy & Access to Information

**Purpose:**

The purpose of this Policy is to confirm the Carleton University's (the University) continued commitment to the principles of access to information (whether personal or institutional) and protection of privacy in light of access to information or protection of privacy statutes and regulations that may apply to the University ("**Applicable Access and Privacy Legislation**").

**Scope:**

1. This Policy, its Schedules, and of any procedures established pursuant to it applies to all Members of the University Community. "**Members of the University Community**" includes but is not limited to:
  - a) employees, including all unionized and non-unionized academic and support staff as well as those whose salary is paid through sources other than the University's operating funds, such as grants, research grants and external contracts;
  - b) adjunct, visiting and emeritus professors; post-doctoral or clinical fellows; and research trainees;
  - c) contractors, consultants, suppliers or other entities engaged by the University to provide services or goods when on University property or while acting in a capacity defined by their relationship to the University;
  - d) members of the Board of Governors, of the Senate and any of their respective committees, as well as members of any advisory committee formed to help the University achieve its goals;
  - e) employees of both unionized and non-unionized employee and student groups when on University property or while acting in a capacity defined by their relationship to the University; and
  - f) visitors, including visiting students and volunteers or persons who serve on advisory or other committees.
2. This Policy does not apply to Personal Health Information. Matters related to Personal Health Information are subject to the Policy on Personal Health Information Processing.

**Interpretation:**

1. Carleton University is subject to Ontario's *Freedom of Information and Protection of Privacy Act* ("**FIPPA**") and regulations thereunder. This Policy is not intended to restate the provisions of FIPPA or any other Applicable Access and Privacy Legislation. However, the provisions of this Policy and any procedures established pursuant to it shall be read in a manner that is consistent with the University's obligations under Applicable Access and Privacy Legislation.
2. This Policy shall read in conjunction with other instruments that may, in certain circumstances, govern access to information and protection of privacy matters, including collective agreements, information security policies, and records management policies.
3. This Policy shall be read in conjunction with any directives, guidelines and procedures that are established concerning access to information and protection of privacy.
4. Upon approval of this Policy, the following policies are considered repealed and have no further effect;
  - a) Policy on Access to Information and Protection of Privacy, April 2014
  - b) Policy on Collection of Personal Information, April 2014
  - c) Policy on Head of the Institution and Delegation of Authority, April 2014
  - d) Policy on the *Personal Information Protection and Electronic Documents Act, Canada* (PIPEDA), November 2013
5. Upon approval of this Policy, the following policies are considered repealed and form part of this Policy's schedules;
  - a) Policy on Freedom of Information Fee Schedule, April 2014
  - b) Policy on Student and Applicant Record, April 2014

**Definitions:**

For the purposes of this Policy and of any directives, guidelines and procedures established pursuant to it:

**"Privacy Breach"** means the loss of, unauthorized access to, or unauthorized disclosure of, Personal Information under the University's custody or control. Situations that may result in a Privacy Breach include the theft or loss of a computing device including mobile devices containing Personal Information or accessing Personal Information that is not required for performance of one's work duties.

**"Personal Information"** means recorded information about an identifiable individual, including the individual's address, sex, age, education, medical or employment history and other information about the individual under the University's custody or control as provided in FIPPA.

**"Record"** means information created, received and maintained, regardless of medium and format, for evidentiary, transactional, or informational value by the University in pursuit of legal obligations or business activities.

Any other capitalized words or expressions used in this Policy are defined for the purposes of this Policy and any procedures established pursuant to it.

**Roles and Responsibilities:**

1. The General Counsel of the University shall be responsible for oversight of access to information and privacy matters at the University.

2. Reporting to the General Counsel of the University, the Manager handles access to information requests, investigates Privacy Breaches, and responds to privacy complaints. The Manager also carries out the following associated duties:
  - a) ensure the University's compliance with FIPPA, its regulations and other Applicable Access and Privacy Legislation;
  - b) oversee the operational responsibilities of the Privacy Office;
  - c) develop and deliver awareness and training sessions on access to information and privacy;
  - d) exercise delegated powers and duties under FIPPA;
  - e) advise Members of the University Community on access to information and privacy matters;
  - f) establish and review privacy policies, notices, guidelines, and processes across the University;
  - g) conduct privacy impact assessments, or review privacy impact assessments developed by project managers;
  - h) lead the response of a Privacy Breach;
  - i) report on activities and statistics relevant to the access to information and privacy to the Senior Management Committee;
  - j) prepare and submit the University's annual report as required under FIPPA;
  - k) maintain a directory of Personal Information Banks; and
  - l) represent the University in interactions with the Information and Privacy Commissioner of Ontario.
3. For the purposes of FIPPA, the "head" or individual responsible for compliance with the requirements of FIPPA is the President of the University. The President delegates to the General Counsel of the University and to the Manager all powers and duties related to the University's compliance with the requirements of FIPPA. The President may appoint an alternate delegate in case the General Counsel and/or the Manager are unable to exercise powers or carry out duties so delegated. All such delegations are pursuant to FIPPA and do not in any way limit the authority of the President as the designated "head" under FIPPA from exercising any of the powers or carrying out any of the duties so delegated.
4. The University Registrar shall be the custodian of all applicant and registered student information.
5. Members of the University Community shall take all reasonable measures to prevent the occurrence of a Privacy Breach.
6. Members of the University Community must cooperate and assist the Privacy Office as required in the fulfillment of the University's obligations under this Policy, related procedures and Applicable Access and Privacy Legislation.

## **Policy**

### **1. Access to Information**

- a) The University routinely makes large amounts of its institutional information available to the public on the University's website. If desired information is not available on the University's website, a request for information may be made to the University's Privacy Office to the attention of the Manager, Privacy & Access to Information ('the Manager') pursuant to the 'Requesting Access to Information Procedure' and the 'Freedom of Information Fee Schedule'.

## 2. Privacy

- a) The University is committed to maintaining and protecting the integrity of Personal Information and confidential information in its custody or control.
- b) If a person believes his or her privacy rights have been violated, the person may file a written complaint with the Manager, who, in turn, shall investigate the complaint.
- c) Members of the University Community shall report a Privacy Breach (whether confirmed or suspected) to the Privacy Office and the Privacy Breach shall be handled in accordance with the University's 'Privacy Breach Reporting Protocol'.

## 3. Notice Of Collection Of Personal Information

Personal Information submitted to the University by a student, employee, alumni, donor or other individual is collected under the authority of the *Carleton University Act, 1957*, and is intended to be used for the purposes of and those consistent with the administration of University programs and activities and in order to carry out other University services and functions, including without limitation the following:

- recruitment, admission and registration, academic programs and evaluations, and graduation;
- evaluation of academic and non-academic programs;
- assistance to student associations, retiree associations and the University's Alumni Association;
- financial assistance, awards and payment of fees;
- alumni and development activities;
- institutional planning and statistics;
- centralization or sharing of service delivery among academic units, administrative services and programs;
- reporting to government agencies, funding agencies and professional licensing bodies;
- fulfillment of requirements related to affiliated institutions;
- employment related matters;
- safety and security;
- detection, monitoring and prevention of non-compliance with policies, regulations and procedures; and
- promotion in print, electronic and internet publications.

The University may collect the minimum amount of Personal Information about a student, employee, alumnus, donor or other individual that is publicly available on the Internet, in social media or in any other medium and that is necessary for its needs and for the proper administration or discharge of its functions or lawful activities, including without limitation:

- planning, review or delivery of programs or services;
- research and statistical activities; and
- compliance with policies, procedures and regulations.

The University is required to disclose Personal Information such as Ontario Education Numbers, student characteristics and educational outcomes to the Minister of Training, Colleges and Universities pursuant to section 15 of the *Ministry of Training, Colleges and Universities Act*, R.S.O. 1990, c. M. 19, as amended. The Ministry collects this information for purposes such as planning, allocating and administering public funding to

colleges, universities and other post-secondary educational and training institutions, as well as research and analysis (including longitudinal studies) and statistical activities conducted by or on behalf of the Ministry in relation to post-secondary education and training. Further information on how the Ministry uses this Personal Information is available on the Ministry's website.

Questions by an individual regarding the collection and use of their own Personal Information in a particular instance should be addressed to the University academic office, administrative office or service responsible for such collection and use. Questions of a general nature regarding the collection, use and disclosure of information should be addressed to the University's Manager, Privacy & Access to Information, by email at [university\\_privacy\\_office@carleton.ca](mailto:university_privacy_office@carleton.ca), by telephone at 613-520-2600 extension 2047, or by mail at Carleton University, Privacy Office, 607 Robertson Hall, 1125 Colonel By Drive, Ottawa, ON, K1S 5B6.

#### **4. Disclosure of Personal Information**

The University shall not disclose Personal Information to external individuals or organizations unless,

- a) otherwise provided by the Notice of Collection of Personal Information in this Policy;
- b) the individual is notified of such potential disclosure when the Personal Information is collected;
- c) the individual has consented to the disclosure; or
- d) permitted under Applicable Access and Privacy Legislation or by law.

#### **5. Information Collected For Public Purpose**

The University considers the following information as information collected and maintained for the purpose of creating a record that is available to the public and that may be published in print, electronic format or on the Internet:

- a) the degree or degrees conferred by the University and the date received; and
- b) the recipient of excellence scholarships or other prizes or honours awarded by the University or a third party.

#### **6. Access to, and Correction of, Personal Information**

Individuals have a right to request access to, and correction of, their own Personal Information. Requests for access to, or correction of, an individual's own Personal Information shall be directed in the first instance to the academic office, administrative office or service that is likely to have the information. In circumstances where such a request does not yield satisfactory results, a further request for access or correction may be directed to the Manager.

#### **7. Personal Information Banks**

As required by FIPPA, the Privacy Office maintains an index of Personal Information Banks (PIBs) which outlines all academic and administrative offices or services that create and maintain Personal Information Banks for purposes of carrying out University services or functions. The index of Personal Information Banks shall be published on the Privacy Office's web site.

## **8. Retention and Disposal of Personal Information**

The records retention schedule established by the University's Corporate Archives sets out the University's practices regarding the retention and disposal of records. If the Carleton University Retention Schedule does not provide for rules for retention and disposal for specific classes of Personal Information, the University shall retain the Personal Information for a minimum of one year after last administrative use. The exception is when the individual to whom the information relates consents to its earlier disposal.

## **9. Mandatory Training**

Members of the University Community who handle Personal Information under the custody or control of the University must complete mandatory access to information and protection of privacy training, relevant to their role, as determined by the University.

### **Implementation, Review and Amendment**

1. The General Counsel of the University is responsible for periodic review of this Policy.
2. Amendments to this Policy other than those set out in paragraph (3) below shall require the approval of the Senior Management Committee.
3. The General Counsel of the University may amend this Policy in order to update the following information contained herein:
  - a. the designation, title or identity of officials, offices, or departments and contact information within the University;
  - b. the designation or title of government ministries or agencies;
  - c. the title or citation of legislation, regulations, policies or procedures.
4. The General Counsel of the University may establish, amend, abrogate or make exceptions to procedures for purposes of the effective implementation of this Policy, provided that such procedures or exceptions are consistent with the provisions of this Policy.

### **Contacts:**

Questions related to the administration of this Policy should be directed to;

- Carleton University Privacy Office  
607 Robertson Hall  
613-520-2600, extension 2047  
[university\\_privacy\\_office@carleton.ca](mailto:university_privacy_office@carleton.ca)

### **Schedules:**

- Schedule 1 – Freedom of Information Fees
- Schedule 2 – Student and Applicant Records

### **Links to related Policies:**

- Corporate Records and Archives Policy
- Data and Information Classification and Protection
- Information Security Incident Response
- Information Technology (IT) Security
- Mobile Technology Security
- Password Policy for Information Systems
- Personal Health Information Processing Policy

## Schedule 1 – Freedom of Information Fees

**Purpose:**

The purpose of this Schedule is to set fees to be charged when processing formal requests for information under FIPPA.

**Interpretation:**

1. The University shall use the Schedule of Fees below when processing formal access requests under FIPPA.
2. A fee estimate will be provided for your agreement when the fees are expected to exceed twenty-five (\$25) dollars.
3. The University shall not charge fees for a formal access request when the total chargeable fee is twenty (\$20) dollars or less.
4. Informal access requests are not subject to the FIPPA fee schedule. They are subject instead to the University's regular reproduction and service fees.
5. Fees for search and preparation cannot be charged when the request is for access to the individual's own personal information.
6. The University shall continue to charge its regular fee for an official transcript or other records where an established procedure exists to provide routine access.
7. Fees will be charged for goods and services for which the University incurs providing access to information for your request.
8. The University may require the requestor to pay 50% of the total estimated fee if it is \$100 or more.
9. The University must refund any fee deposit paid that is subsequently waived or not used.
10. Efforts will be made to keep fees reasonable and accessible.

**Fee Schedule:**

Action	Fees
Making an access request	\$5 fee must accompany formal written request
Change in Personal Information	No fee required
Photocopies and computer printouts	\$0.20 per page
CDs, DVDs, USB Drives	\$10 per media
Manually searching for a record	\$7.50 for each 15 minutes spent by any person
Preparing a record for disclosure, including severing part of the record	\$7.50 for each 15 minutes spent by any person
Developing a computer program or other method to produce a record from a machine-readable record	\$15 for each 15 minutes spent by any person
Use of external services and shipping companies to respond to a request	Actual costs

## Schedule 2 – Student and Applicant Records

### Purpose:

- To define the rights and obligations of students and of the University and its officers in matters pertaining to student records and applications.
- This Schedule should guide the Registrar's Office, Graduate Studies Registrar's Office, Recruitment and Admissions, academic units, Awards and Financial Aid, Awards (Graduate Studies), Alumni and Advancement and all other primary and secondary custodians of data collected and stored about all applicants, students, and former students in degree programs, and certain non-degree programs, for the University.
- Any employee who occasionally and for specific purposes has access to the student record (regardless of format) will also adhere to this policy.

### Procedures:

#### A. Electronic Information and Networked Information

- Access to retrieve and manipulate data through our information systems will only be provided to those requiring such access as part of their job descriptions at the University.
- The Department Heads, Deans, and Directors will be responsible for delegating authority to access student records. The responsibility for due diligence rests upon these authorized users to ensure appropriate use and confidentiality of student and applicant information.
- Faculty and staff must use electronic communication with sensitivity and due diligence for the protection of students. Electronic communication that contains personal information (eg. Grades) should only be undertaken via official Carleton email systems (i.e. CUNET or CMAIL accounts, or electronic teaching systems such as the University's Learning Management System (LMS)).
- In all cases, the protection of privacy will take priority over administrative efficiency.
- The gathering of personal information (beyond the class lists) by individual instructors must be preceded by a signed release form from the students registered in the class.

#### B. Information Contained in Student Record

The University shall collect no more information than it needs and the minimal amount of additional information required to accomplish a legitimate institutional purpose. The University will explain the purpose for which it collects information at the time of collection and will request authorization to release certain personal information externally where applicable. Where not possible the University will have confidentiality agreements signed with these third-parties.



The printed student record may consist of but is not limited to the following information:

- Biographical information (name, address, email address, telephone, date of birth, citizenship, next of kin, social insurance number, student number, photograph, signature, etc.)
- Admission information (application, record of previous studies, letters of recommendation, test results, etc.)
- Enrolment information (program of study, dates of attendance / registration, courses taken, student number)
- Performance information (examination results, evaluations; narrative and clinical, distinctions, sanctions, degrees obtained)
- Results from petitions and appeals filed by the student
- Medical information relevant to a student's performance, provided both by request or with the consent of the student
- Financial information (charges, payments, awards, debts, etc.)

The electronic student record may consist of but is not limited to the following information:

- Biographic (name, address, student number, social insurance number, photograph, signature, etc.)
- Academic (basis of admission, degree program, concentration, courses enrolled, transferred credits, rulings, grades, averages, ranks)
- Financial information (tuition fees, debts, scholarships and awards)

### **C. Storage and Retention of Records**

- The University maintains and preserves student records in hard copy and electronic form
- Electronic records contain all information to monitor and administer the progress and performance of students, produce reports, and provide official transcripts of the academic record. They are also used to administer the operation of the University (enrolment reports, statistical information, and report to government agencies).
- All portions of the student electronic record required to produce official transcripts are maintained permanently. These records will be reviewed and accessed at the time of system upgrade or migration.
- Physical student records are retained and disposed of according to the Carleton University Retention Schedule and the Registrar's Office retention and disposition practices

### **D. Access to Records and Disclosure of Information**

- Personal information contained in the student record may be disclosed according to Sections 21 and 42 of FIPPA.
- A student's registration status is not considered to be public information, and may not be disclosed except in accordance with Section 42 of FIPPA.
- Students may request additional privacy for reasons of personal security (threats or harassment). These requests shall be directed to the Registrar's Office. The electronic record will be marked for additional privacy and authorized use will be limited. In these instances staff access and academic access for official duties will require contact with the Registrar's Office.

- The student number is considered personal information and must be kept confidential according to FIPPA. Its disclosure constitutes an unjustified invasion of personal privacy. (eg. Should not be released over the telephone)
- Grades and evaluative comments are also confidential; instructors should develop a process for returning graded material that does not jeopardize this confidentiality. Best-practice includes developing a LMS course website and having papers returned by the faculty or administrators to students upon presentation of proper identification (eg. Carleton Campus Card).

#### **E. Student Access**

- Students have the right to inspect documents contained in their own record:
  - o This includes the right to view their submissions to final exams but not including the exam questions
  - o The University may refuse to disclose personal information according to Section 49 of FIPPA, that includes exemptions for “evaluative or opinion material” such as confidential evaluations and letters of reference supplied to the University.
- Students have the right to correct information contained in their record. Recipients of incorrect information will be notified of the correction. According to Section 47(2) (b) of FIPPA, a student may “require that a statement of disagreement be attached to the information reflecting any correction that was requested but not made”.
- Students have direct access to their electronic record via Carleton Central for biographic, academic and financial information. If the student wishes to inspect the physical record they should contact the Registrar’s Office for an appointment. This information will only be provided in person or by written request and released only with proper identification (Carleton Campus Card / Student Number)
- A student’s formal request for their own official transcripts will be granted if it is accompanied by the required payment, and their account has no outstanding balance. The student may also request release of this official transcript to a third party however a signed Third Party Release Form must be signed beforehand.
- Students will not be granted access to official documents from other institutions or universities contained in their university record. Students must contact these parties individually and request the information directly.
- Students with a debt to the University may be sanctioned under the Student Accounts with a Debt Balance Policy and denied access to personal information such as official transcripts and may not be able to register. Access may also be denied based on other university policies.

#### **F. Faculty and Staff Access**

- Faculty and staff members of the University are given access to information contained in the official student record on a NEED TO KNOW basis. The University systems database has been designed to mask certain fields of personal information according to work / job duty requirements. Information about students will be provided to employees for performance of their official duties at the University. As a rule, only employees involved in aspects of academic administration or student affairs are given access to student record content.
- Individual instructors are generally not entitled to view any part of the student record unrelated to the administration of their specific course. This includes past academic performance and letters of reference.

#### **G. Student Government Access**

- Students will be notified during registration through the Notice of Collection that their personal information may be provided to the student government. Students have the right to request that their information not be provided to student associations by contacting the Registrar's Office.
- The University and the student associations will sign an agreement stating the use/s of this information and the responsibility and onus for the protection of privacy. If new uses of personal information arise, an amendment must be signed and attached to the agreement. The agreement shall be reviewed annually.
- Students become members of the Carleton University Student Association or the Graduate Student Association (GSA and CUSA) upon the payment of their student activity fees. Students may opt out of certain fees that will deny them access to specific services and activities. The University may provide the student government lists for the purpose of identifying eligibility for some services.

#### **H. Legally Mandated Access**

- Specific records or portions of these records may be provided to:
  - o Persons or agencies pursuant to a court order, summons, or subpoena directing the University to release information;
  - o To the Ministry of Education and the Ministry of Training, Colleges and Universities in connection with enrolment audits and fraud;
  - o To Statistics Canada for national surveys;
  - o In accordance with the requirements of duly constituted professional licensing and certification bodies;
  - o In accordance with Section 42 (1) of FIPPA.