Durham College Policy and Procedure

TYPE:	Administrative
TITLE:	Access to Records and Protection of Privacy
NO.:	ADMIN-222
RESPONSIBILITY:	Chief Administrative Officer
APPROVED BY:	Durham College Leadership Team
EFFECTIVE DATE:	October 2019
REVISED DATE(S):	
REVIEW DATE:	October 2022

1. Introduction

The Freedom of Information and Protection of Privacy Act (FIPPA) is provincial legislation that applies to Ontario colleges.

Some key purposes of the Act are:

1. To provide the public a right of access to College information subject to limited exemptions; and,

2. To protect the privacy of individuals with respect to personal information about themselves held by the College and to provide individuals a right of access to that information.

Most records in the custody or control of the College are subject to FIPPA and a majority of these records will be available if requested; however, certain records are excluded from FIPPA's application, such as:

1. Most college labour relations or employment records;

2. Records respecting college research, except the subject matter and the amount of funding related to research;

3. Records available to the public or expected to be published within 90 days;

4. College teaching materials.

In some cases, the records held by the College will be also be covered by the Personal Health Information Protection Act (PHIPA) and all requests for records will be reviewed against the appropriate legislation.

This policy and procedure applies to all College Employees, volunteers, agents and contractors.

2. Purpose

The purpose of this policy and procedure is to provide guidance on the collection, use and disclosure of information held by the College; the access to information process and the College's protocol for handling a privacy breach.

3. Definitions

Refer to Durham College's Standard Definitions.

4. Policy statements

4.1. General

4.1.1. The College shall comply with the provisions of FIPPA and the PHIPA.

4.1.2. The College shall identify the purposes for which personal information is collected at or before the time the information is collected through the use of a notice of collection statement.

The College's standard notice of collection is as follows:

In accordance with Section 39(2) of the Freedom of Information and Protection of Privacy Act, 1990, the personal information collected on this form is collected under the legal authority of the Ontario Colleges of Applied Arts and Technology Act, 2002 and may be used and/or disclosed [insert your purpose]. Your personal information may also be used/disclosed for various administrative, statistical and/or research purposes of the College and/or ministries and agencies of the Government of Ontario and the Government of Canada. If you have any questions about the collection, use and disclosure of your personal information by the College, please contact the Freedom of Information and Protection of Privacy Coordinator, 2000 Simcoe Street North, Oshawa, ON, L1G 0C5, 905.721.2000 ext. 3292.

4.1.3. The College shall identify personal information banks in a manner consistent with FIPPA.

4.1.4. The College shall make readily available specific information about its policies and practices relating to the management of personal information.

4.1.5. The Durham College (DC) Board of Governors delegates all powers and duties of the "head" as defined by FIPPA to the Chief Administrative Officer.

4.1.6. For the purposes of PHIPA, the Director, Campus Health Centre is considered the Health Information Custodian for health records held by the Campus Health Centre.

4.1.7. If this policy and procedure is found to in any way conflict with a provision of FIPPA or PHIPA, the provision of FIPPA or PHIPA will take precedence.

4.2. Privacy

4.2.1. The College regards all personal information pertaining to applicants, current Students, former Students, Employees and donors as confidential.

4.2.2. The College shall protect personal information by security safeguards appropriate to the sensitivity of the information.

4.2.3. The College will dispose of records containing personal information in a secure manner in accordance with the College's common records schedule.

4.3. Use of Personal Information – Student

4.3.1. By applying for admission to the College and by enrolling in a program at the College, Students consent to the collection of their personal information by the College for educational, administrative and statistical purposes. The information is needed to process admission applications and enrolment and registration in academic programs; to record and track academic progress; to provide the basis for awards and government funding, and for related recordkeeping purposes.

4.3.2. By applying for admission to the College through the Ontario College Application Service (OCAS) and enrolling in a program, the College has consent to use a Student's personal information for communication of information relating to events, activities, fee payment reminders and other commercial messaging specific to the College.

4.4. Web Privacy Guidelines

4.4.1. The College may use personal information for marketing material or for your subscription to College mailing lists, only with an individual's knowledge and consent. The College may also use information to respond to questions asked, process website requests, allow participation in contests, and announce special events.

4.4.2. The College collects non-identifiable information through website technology such as cookies and web server files. Cookies allow users to have a better experience and improve site navigation by storing information on a user's machine that can later be retrieved. The College uses this information to gain accurate visitation statistics. Visitors may reject any or all cookies by using their web browser's preferences. Please note, certain features of the website may require the use of cookies in order to function properly, such as forms. Web server log files provide statistical information such as traffic patterns by recording your IP address, login ID, date and time you visit the site, and the webpage that referred you to the site.

4.4.3. The College may also use a third-party service provider to serve ads on our behalf across the Internet. They may collect anonymous information about your visits to our website, and your interaction with our programs and courses. They may also use information about your visits to this and other websites to target advertisements for our programs, courses and services. This anonymous information is collected through the use of a pixel tag, which is industry standard technology used by most major websites. No identifiable information is collected or used in this process. They do not know your name, phone number, address, email address, or any identifying information about you.

4.4.4. All companies that act on the College's behalf are contractually obligated to keep the information we provide to them confidential and to use the information we share only to provide the services we ask them to perform.

4.4.5. The College may report on statistical information gathered from the above resources but will not sell, trade, lend or willingly disclose any of your personal information to any third party companies.

4.5. Routine Disclosure

4.5.1. The College will disclose, outside of the formal FIPPA process, the following records upon request as long as the requester is entitled to have the information or where required, a Consent to Release Form has been completed:

a) The names and biographies of the College's Board of Governors;

b) Public minutes of the Durham College Board of Governors meetings;

c) Public minutes of the Durham College Board of Governors, Governance Review Committee meetings;

d) The College's annual report, business plan and strategic plan;

e) The College's approved strategic mandate agreement;

f) General program and course information;

g) Other College documents publicly available on the College website;

h) Information about a College Employee in their professional capacity (e.g. name, title, College email address);

i) Whether or not a Student has received a particular academic award, honour or distinction whether from Durham College or an external third-party;

j) Whether or not a Student has received a diploma(s) or credential(s) conferred by Durham College and the date(s) of conferral;

k) Student records such as transcripts, letters of verification, official receipts, tuition tax forms, duplicate credentials;

l) Verification of employment or employment records.

4.6. Disclosure of Personal Information to Other Parties

4.6.1. The College will only disclosure personal information consistent with the provisions of FIPPA and/or PHIPA.

4.6.2. Personal information may be shared with the following parties to facilitate fundamental activities:

a) Other post-secondary institutions to verify any information provided as part of an application for admission;

b) Other universities and colleges to share incidences of falsified documents or credentials, or to share information regarding fraudulent applications for admission;

c) Government offices to verify information regarding an application for admission and to support processes for government financial aid;

d) Other universities and colleges with which Durham College maintains a collaborative program partnership;

e) Service providers contracted by Durham college to support business processes;

f) Government agencies federal and provincial, and law enforcement agencies relating to international Student programs, study visas and other immigration matters, or for matters of national security or non-compliance with federal and provincial regulations.

4.6.3. The College will disclose personal information to the Ministry of Training, Colleges and Universities and Statistics Canada, as required.

5. Procedure

5.1. Informal Requests for Information

5.1.1. A formal access request under FIPPA will not be required if the information is routinely disclosed by the College as part its regular business practices as noted Section 4.5.1.

5.2. Requests for Student or Employment Records

5.2.1. Requests for Student records should be processed in accordance with the College's policy/procedure on Access to Student Records and Protection of Privacy.

5.2.2. Requests for access to Student records received directly from a Student or individual (e.g. parent or legal guardian) designated by a Student through the completion of a Consent to Release Form, or alumnus/a are to be handled by Strategic Enrolment Services.

5.2.3. Requests for access to Student records by a third party agent (ex. lawyer's office or insurance company) are to be directed to the Freedom of Information and Protection of Privacy Coordinator.

5.2.4. Requests for access to employment records authorized by the Employee are to be handled by Human Resources.

5.3. Requests for Personal Health Information

5.3.1. The Director, Campus Health Centre is responsible for responding to requests for personal health information and the annual reporting to the Information and Privacy Commission.

5.3.2. To request personal health information, a written request must be sent to the Campus Health Centre and the request will be processed according to relevant legislation and the procedures established by the Campus Health Centre.

5.3.3. The Campus Health Centre complies with the provisions of the Personal Health Information Protection Act, and will only release documents in compliance with the Act.

5.4. Formal Requests for Information

5.4.1. Method of Request - all requests are to be made in writing using the Durham College Application for Access/Correction of Records Form and directed to the attention of the Freedom of Information and Protection of Privacy Coordinator.

- When a request is made to another department or entity at Durham College, the requestor should be directed to contact the Freedom of Information and Protection of Privacy Coordinator.

5.4.2. Payment of Request Fee – In accordance with section 24(1)(c) of FIPPA, all requests must be accompanied by a fee of $5.00 payable by cash, cheque or money order.

5.4.3. Contact with the Requestor – Any and all contact with the requestor shall be conducted by the Freedom of Information and Protection of Privacy Coordinator.

a) The Freedom of Information and Protection of Privacy Coordinator will communicate with the requestor as needed to clarify the request or otherwise respond to the request.

5.4.4. Fees & Fee Estimates – In accordance with section 57 of FIPPA, Durham College will charge the requestor fees for the costs of (a) searching for records, (b) preparing the records for disclosure, (c) locating, retrieving, processing and copying the records, (d) shipping costs, and (e) any other costs incurred in responding to the request.

a) The fees charged shall be calculated according to the values set out in section 6 of the General Regulations to FIPPA.

b) In accordance with section 57(3) of FIPPA, a fee estimate will be issued to the requestor when the fees are expected to be over $25.00.

c) In accordance with section 7(1) of the General Regulations to FIPPA, a requestor will be required to pay a 50 per cent deposit of the amount of the fee estimate when the fee estimate is an amount greater than $100.00.

d) In accordance with section 9 of the General Regulations to FIPPA, a requestor must pay the entirety of the fees due before they are provided with responsive records.

e) All fees are to be paid to Durham College and collected by the Freedom of Information and Protection of Privacy Coordinator.

5.4.5. Collection of Records – Upon receipt of a request, the Freedom of Information and Protection of Privacy Coordinator will review the request and collect all potentially relevant records.

a) Where potentially responsive records are held by departments or entities other than the Freedom of Information and Protection of Privacy Coordinator, the Freedom of Information and Protection of Privacy Coordinator will co-ordinate with those other departments or entities to properly search for and locate all potentially responsive records.

b) Steps undertaken by other departments or entities to search for records must be documented and a summary provided to the Freedom of Information and Protection of Privacy Coordinator for their records.

5.4.6. Notices to Affected Parties – In accordance with section 28 of FIPPA, the Freedom of Information and Protection of Privacy Coordinator shall notify all affected parties and solicit representations from (a) third parties to whom information in the records relates and to which the section 17 exemption may apply; or (b) individuals whose personal information is contained in the records if disclosure of that personal information might constitute an unjustified invasion of personal privacy.

a) The Freedom of Information and Protection of Privacy Coordinator must give full and fair consideration to the representations of any affected third parties but ultimately remains responsible for rendering an access decision.

5.4.7. Time Extensions – The Freedom of Information and Protection of Privacy Coordinator may issue a time extension in three circumstances:

a) In accordance with section 27(1)(a) of FIPPA where the request is for a large number of records or necessitates a search through a large number of records and meeting the time limit would unreasonably interfere with the operations of the institution;

b) In accordance with section 27(1)(b) of FIPPA where consultations with a person outside the institution are necessary to comply with the request and cannot reasonably be completed within the time limit;

c) In accordance with section 28(4) of FIPPA where notice has been given to an affected party and that party is to be afforded the opportunity to make representations.

5.4.8. Application of Exclusions & Exemptions – The Freedom of Information and Protection of Privacy Coordinator has sole responsibility for applying all relevant exclusions or exemptions to the potentially responsive records.

a) Where an exemption is discretionary the Freedom of Information and Protection of Privacy Coordinator is designated the authority to exercise the appropriate discretion.

5.4.9. Decisions – The Freedom of Information and Protection of Privacy Coordinator is designated the power to issue a final access decision.

5.4.10. Appeals – Where a requestor appeals any aspect of a decision to the Information and Privacy Commissioner, the Freedom of Information and Protection of Privacy Coordinator is responsible for coordinating Durham College's participation in and response to any such appeal.

5.4.11. Record Keeping – the Freedom of Information and Protection of Privacy Coordinator will maintain a record of all access requests, decisions and appeals for a period of 5 years after the file is closed.

5.5. Privacy Breach Protocol

The College's privacy breach protocol is applicable to all personal information held by the institution, regardless if the record is covered by FIPPA or PHIPA. If the personal information breached is related to personal health information then the Freedom of Information and Protection of Privacy Coordinator will work with the Director, Campus Health Centre to respond to the breach appropriately.

When a privacy breach is alleged to have occurred or an Employee, volunteer, agent or contractor otherwise believes a privacy breach may have occurred, immediate action should be taken.

In all instances of a potential privacy breach, the following steps, conducted in quick succession or concurrently, shall be followed:

5.5.1. Step 1: Identification and Alert

a) Upon the identification of a potential privacy breach, the Employee, volunteer, agent or contractor shall notify a supervisor or manager who shall in turn notify the Freedom of Information and Protection of Privacy Coordinator.

b) If a supervisor or manager is unavailable, the Employee, volunteer, agent or contractor should contact the Freedom of Information and Protection of Privacy Coordinator directly to report the potential privacy breach.

c) The following information, if known, will be helpful when reporting a potential breach:

- The nature of the personal information involved (e.g. name, social insurance number, etc.);
- The number (potential or actual) of individuals affected by the potential breach and who they are (e.g. Employees, Students);
- The possible scope of the breach (e.g. internal/external – who might have gained access to the personal information without consent or authorization, length of time before detection of breach, etc.);
- The date and/or location of the incident giving rise to the breach;
- When and how the breach was discovered.

d) The Freedom of Information and Protection of Privacy Coordinator will review and assess all relevant facts to determine if a privacy breach has occurred from the College's perspective.

e) If the breach involves data related to a shared service with DC and the University of Ontario Institute of Technology (UOIT), the Freedom of Information and Protection of Privacy Coordinator will notify UOIT as soon as practicable.

If it is determined that a privacy breach has occurred, the Freedom of Information and Protection of Privacy Coordinator will proceed with Steps 2 to 4.

5.5.2. Step 2: Containment

The Freedom of Information and Protection of Privacy Coordinator shall, in conjunction with the relevant department, undertake the following actions to contain the privacy breach:

- Retrieve and secure any records associated with the breach and retrieve hard copies of any personal information that has been disclosed;
- Where appropriate and depending on circumstances, isolate and suspend access to any system associated with the breach;
- Ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information;
- Determine if the privacy breach would allow unauthorized access to any other personal information (e.g. an electronic information system) and take any necessary steps (e.g. change passwords, temporarily shut down a system);
- Take any other action necessary to contain the breach.

5.5.3. Step 3: Notification

The Freedom of Information and Protection of Privacy Coordinator shall:

a) Notify the President, the Chief Administrative Officer and the relevant Vice-President in writing of the privacy breach. The Chair of the Board of Governors (the "head" as defined in the legislation) shall be notified if the breach is reported to the Information and Privacy Commission (IPC).

b) Except in the case of personal health information, the College is not legally obligated to notify the IPC of a privacy breach, and therefore will notify the IPC when:

   a) A privacy breach involving the personal health information of one or more individuals has occurred; or

   b) When the breach involves the personal information of one or more individuals and the Freedom of Information and Protection of Privacy Coordinator considers it appropriate to do so based on consideration of what is best for the individual(s) affected and the following factors:

- The number of individuals affected;
- The nature of the breach;
- The scope of the breach;
- Whether the breach has been fully resolved;
- The College's need for IPC guidance in responding to the breach;
- Any other factors that are relevant to the Coordinator.

c) Notify the individuals whose privacy was breached, by telephone or in writing and:

a) Provide details of the extent of the breach and the specifics of the personal information at issue;

b) Advise of the steps taken to address the breach, both immediate, and long-term (if known);

c) Advise they may make a complaint to the IPC and provide the contact information for the IPC.

5.5.4. Step 4: Investigate and Conclude

The Freedom of Information and Protection of Privacy Coordinator shall:

a) Conduct an internal investigation to ensure the immediate requirements of containment and notification have been addressed, to review the circumstances surrounding the breach, and to review the adequacy of existing policies and procedures in protecting personal information.

b) If required, prepare a breach report for submission to the IPC and cooperate in any further investigation into the incident undertaken by the IPC.

c) Ensure Employees, volunteers, agents and contractors are appropriately educated and trained with respect to the privacy provisions of FIPPA.

6. Roles and responsibilities

6.1. Under the direction of the Chief Administrative Officer, the Freedom of Information and Protection of Privacy Coordinator is responsible for:

a) Receiving and assessing requests for information (excluding personal health information) and determining the correct process for accessing the information;

b) Forwarding the request to the relevant Vice-President, Director or Manager for delegation and action, and monitoring the progress of the response to ensure compliance with FIPPA;

c) Applying all relevant exclusions or exemptions to potentially responsive records and issuing an access decision;

d) Requesting time extensions when necessary and coordinating third party notifications were appropriate;

e) Issuing fee notices, collecting deposits, and collecting all outstanding fees before releasing records;

f) Training College Employees on the College's policies and procedures relating to FIPPA and on FIPPA itself;

g) Acting as a resource for College Employees tasked with the responsibility of compiling responses;

h) Preparing reports relating to access requests as required by the government; and,

i) Responding to all potential or actual privacy breaches pursuant to the protocol described in this policy/procedure.

6.2. Members of the Durham College Leadership Team are responsible for ensuring their departments are complying with the College's policies and procedures related to access and privacy and for providing the resources necessary to respond within the prescribed timeframes when a formal access request is received.

6.3. The Director, Campus Health Centre is responsible for responding to all access requests for personal health information and working with the Freedom of Information and Protection of Privacy Coordinator to report and respond to any privacy breach involving personal health information. The Director, Campus Health Centre is also responsible for submitting annual reports to the Information and Privacy Commission with respect to personal health information.

6.4. The Office of Strategic Enrolment Services is responsible for processing all requests for Student records made directly by a Student or to an individual designated by a Student through the completion of a Consent to Release Form.

6.5. Human Resources is responsible for processing all requests for employment records authorized by an Employee.

6.6. All College Employees, volunteers, agents and contractors are responsible for complying with the College's policies and procedures related to access and privacy and for reporting all instances of a suspected privacy breach.

7. Accessibility for Ontarians with Disabilities Act considerations

Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this policy and procedure and it adheres to the principles outlined in the College's commitment to accessibility as demonstrated by the Accessibility Plan (ADMIN-203).

8. Non-compliance implications

8.1. Non-compliance with FIPPA may result in investigation by the IPC of Ontario, and a penalty not to exceed $5,000 if found guilty of an offence.

8.2. Other implications could include a negative impact on College finances, damage to the College's reputation, human rights challenges or potential legal action against the College.

9. Communications plan

- A message will be posted on ICE alerting Employees when new or revised policies and procedures are added to ICE.
- A message will be posted on MyCampus alerting Students when new or revised policies and procedures are added.

10. Related forms, legislation or external resources

- Freedom of Information and Protection of Privacy Act
- Personal Health Information Protection Act
- Application for Access/Correction of Records Form