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:	April 2022
REVISED DATE(S):	
REVIEW DATE:	April 2025

1. Introduction

The Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Protection Act (PHIPA) are pieces of provincial legislation that apply to Ontario colleges. Subject to limited exemptions, these laws provide the public with a right of access to information held by Durham College (DC). They also carry an obligation for the College to protect individuals' privacy and provide individuals with access to information about themselves.

2. Purpose

The purpose of this policy and procedure is to provide a framework for the collection, use, and disclosure of information held by the College and to explain processes for gaining access to information and handling a privacy breach.

3. Definitions

Refer to Durham College's Standard Definitions.

4. Policy statements

4.1. The College shall comply with the FIPPA and the PHIPA.

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

4.3. Students and employees have the right to access, review and request corrections to their records.

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

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

4.6. The DC Board of Governors delegates all powers and duties of the "head" as defined by FIPPA to the Chief Administrative Officer.

4.7. For PHIPA, the Director, Campus Health and Wellness Centre, is the Health Information Custodian for health records held by the Campus Health and Wellness Centre.

4.8. DC regards all personal information about applicants, current and former students, current and former employees, and donors as confidential.

4.9. DC will protect personal information by security safeguards appropriate to the sensitivity of the information.

4.10. DC may only collect and use personal information with an individual's knowledge and consent. By applying for admission to DC and enrolling in a program at DC, students consent to collecting and using their personal information.

4.11. DC may collect non-identifiable information through website technology such as cookies and web server files.

5. Procedure

5.1 Collection of Personal Information and Web Privacy Guidelines

5.1.1. The College may collect information for educational, administrative, and statistical purposes and use it for commercial messaging specific to the College. Information collected may also be used for activities including, but not limited to: event promotion; reminders of fee payment due dates; providing responses to questions asked; processing website requests; and/or facilitating participation in contests.

5.1.2. Certain features of the DC website require cookies to function correctly. Non-identifiable information collected through cookies or web server files may be used to determine accurate website visitation statistics.

5.1.3. DC may use a third-party service provider to provide online advertising on its behalf. Third-party service providers may collect anonymous information about visits to DC's website and use this information to target advertisements for DC's programs, courses, and services.

5.1.4. All third-party service providers that act on the College's behalf must keep confidential information provided to them by DC and use that information only to provide services the College has contracted them to perform.

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

5.2 Student Access to Their Own Personal Information

5.2.1 Students can access and review records about themselves held by DC, except student evaluations, documents pertaining to academic achievement at other institutions, and letters of reference supplied by the College.

5.2.2. Students must present valid government-issued photo identification or DC student card to view their records.

5.2.3. Students must view their records in the office responsible for the security and confidentiality of the particular record and under the supervision of an employee of that office. Students may have supervised access to the record electronically when a physical record is not maintained or complete.

5.2.4. Students may request the correction of erroneous information in their records and that any recipients of erroneous information be advised of the correction.

5.2.5. Students may not remove records from their files.

5.3. Employee Access to Student Records

5.3.1. A DC employee may access and use the information contained in a student record if it is required to perform their job duties.

5.3.2. The extent of access to student records will correlate to the employee's job responsibilities, as described in the employee's job description.

5.3.3. Access to student medical records is limited to those employees providing relevant, direct support to the student.

5.3.4. An employee's supervisor may withdraw the employee's access to student records.

5.4. Third Party Access to Student Records

5.4.1. Student records will not be released to parents, guardians, or spouses without prior written authorization by the student to the appropriate school/department. Typically, written authorization will be provided by completing the Consent to Release Information Form.

5.4.2. All other third parties, including law offices, insurance companies, and credit bureaus, requesting access to student records must make a request to DC's Freedom of Information and Protection of Privacy Coordinator.

5.5. Access to Employment Records

5.5.1. The Human Resources & Equity department manages requests for access to employment records authorized by an employee.

5.6. Access to Personal Health Information

5.6.1. Requests for personal health information must be in writing and sent to the Campus Health and Wellness Centre.

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

5.7. Routine Disclosure of Records and Information

5.7.1. 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 Information Form has been completed:

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

b) Public minutes of the DC Board of Governors meetings;

c) Public minutes of the DC 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 that are publicly available on the college website;

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

i) Whether a student has received a particular academic award, honour, or distinction from DC or an external third party;

j) Whether a student has received a credential conferred by DC and the date 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.

5.8. Disclosure of Personal Information to Other Parties

5.8.1. DC may share personal information 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 post-secondary institutions to share incidents of falsified documents or credentials or 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 post-secondary institutions with which DC maintains a collaborative program partnership;

e) Service providers contracted by DC 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.

5.8.2. DC will disclose personal information to the Ministry of Colleges and Universities (MCU) and Statistics Canada.

5.9. Legally Mandated Disclosures of Information

5.9.1. Specified records or portions thereof may be provided to persons or agencies according to a court order where DC must comply with the law and as part of law enforcement investigations or proceedings.

5.10 Disclosure of Information in Emergency or Compassionate Situations

5.10.1. For compassionate reasons or in cases of serious emergencies involving health and safety, DC may disclose a student's personal information to third parties. This will be done by the Office of the Registrar in consultation with the Freedom of Information and Protection of Privacy Coordinator. In such circumstances, DC will inform the student of the disclosure.

5.10.2. Students must provide an emergency contact at the time of registration and are expected to update that information as necessary while enrolled at DC. Emergency contact information can be changed through the student portal.

5.10.3. For compassionate reasons or in cases of serious emergencies involving health and safety, DC may disclose an employee's personal information to third parties. This will be done by the Human Resources & Equity department in consultation with the Freedom of Information and Protection of Privacy Coordinator. In such circumstances, DC will inform the employee of the disclosure.

5.10.4. Employees must provide an emergency contact at the time of employment and are expected to update that information as necessary while employed at DC. Emergency contact information can be changed by contacting the Human Resources and Equity department or via the self-service function of the employee portal.

5.11. Formal Requests for Information

5.11.1. All formal requests are to be made in writing using the DC 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 DC, the requestor should be directed to contact the Freedom of Information and Protection of Privacy Coordinator.

5.11.2. All requests must be accompanied by a fee of $5.00 payable by cash, cheque, or money order.

5.11.3. All contact with a requestor to clarify or respond to a request shall be conducted by the Freedom of Information and Protection of Privacy Coordinator.

5.11.4. DC will charge a requestor fees for searching for records; preparing the records for disclosure; locating, retrieving, processing, and copying the records; shipping costs; and any other costs incurred in responding to the request.

a) The fees charged will align with section 6 of the General Regulations to FIPPA.

b) A fee estimate will be issued to the requestor when the fees are expected to be over $25.00.

c) A requestor will be required to pay a 50 percent deposit of the fee estimate amount when the fee estimate is an amount greater than $100.00.

d) A requestor must pay the entirety of the fees due before they are provided with responsive records.

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

5.11.5. 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) The Freedom of Information and Protection of Privacy Coordinator will coordinate with other departments or entities to 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.

5.11.6. The Freedom of Information and Protection of Privacy Coordinator shall notify all affected parties and solicit representations from third parties to whom the information in the record relates and to which the section 17 exemption may apply; or individuals whose personal information is contained in the records if disclosure of that personal information might constitute an unjustified invasion of personal privacy.

5.11.7. The Freedom of Information and Protection of Privacy Coordinator will give full and fair consideration to the representations of any affected third parties, then render access decisions.

5.11.8. The Freedom of Information and Protection of Privacy Coordinator may issue a time extension 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;
- consultation with others outside the institution is necessary to comply with the request and cannot reasonably be completed within the time limit; and/or
- notice has been given to an affected party and that party is to be afforded the opportunity to make representations.

5.11.9. The Freedom of Information and Protection of Privacy Coordinator is responsible for applying all relevant exclusions or exemptions to the potentially responsive records. Where an exemption is discretionary, the Freedom of Information and Protection of Privacy Coordinator is designated the authority to exercise appropriate discretion.

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

5.11.11. 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 DC's participation in and response to any such appeal.

5.11.12. The Freedom of Information and Protection of Privacy Coordinator will maintain a record of all access requests, decisions, and appeals for five (5) years after the file is closed.

5.12. Privacy Breach Protocol

The College's privacy breach protocol applies to all personal information held by the institution, regardless of whether 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 and Wellness Centre, or designate, to respond to the breach appropriately.

5.12.1. When a privacy breach is alleged or believed to have occurred, immediate action will be taken. In all instances of a potential privacy breach, the following actions will be taken:

Step 1: Identification and Alert

a) Upon identifying a potential privacy breach, the employee, volunteer, agent or contractor shall notify a supervisor or manager, who shall notify the Freedom of Information and Protection of Privacy Coordinator using the Privacy Breach Reporting Form.

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

c) The Freedom of Information and Protection of Privacy Coordinator will review and assess all relevant facts to determine if a privacy breach has occurred.

d) If the alleged breach involves data related to a shared service with DC and the Ontario Tech University, the Freedom of Information and Protection of Privacy Coordinator will notify the university as soon as practicable.

If it is determined that a privacy breach has occurred, the Freedom of Information and Protection of Privacy Coordinator will implement steps 2 through 4 of the process.

Step 2: Containment

The Freedom of Information and Protection of Privacy Coordinator, in conjunction with the relevant department, will:

1. retrieve and secure any records associated with the breach and retrieve copies of any personal information that has been disclosed;

2. where appropriate and depending on circumstances, isolate and suspend access to any system associated with the breach;

3. ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information;

4. 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 including, but not limited to, changing passwords or temporarily shutting down a system; and

5. take any other action necessary to contain the breach.

Step 3: Notification

The Freedom of Information and Protection of Privacy Coordinator shall:

1. 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 shall be notified if the breach is reported to the Information and Privacy Commission (IPC).

2. The College will notify the IPC, as legally required, when:

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

    b) 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 an assessment of what is best for the individual(s) affected, accounting for:

        - 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; and/or
        - Any other factors considered relevant.

3. Notify the individual(s) 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 the individual(s) that they may make a complaint to the IPC and provide the appropriate contact information.

4. In the case of records pertaining to the Ontario Student Assistance Program (OSAP), notify the Minstry of Colleges and Universities and law enforcement (if necessary).

Step 4: Investigate and Conclude

The Freedom of Information and Protection of Privacy Coordinator shall:

1. 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;

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

3. Ensure employees, volunteers, agents, and contractors are appropriately educated and trained concerning privacy provisions.

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 according to the

protocol described in this policy/procedure.

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

6.3. The Director, Campus Health and Wellness 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 IPC concerning personal health information.

6.4. The Office of the Registrar 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. The Human Resources & Equity department 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 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 Multi-Year Accessibility Plan.

8. Non-compliance implications

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

8.2. Other non-compliance implications may include a negative impact on College finances, damage to the College's reputation, human rights challenges, or other potential legal actions against the College.

9. Related forms, legislation or external resources

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