Durham College Policy and Procedure

TYPE:	Administrative
TITLE:	Access to Records and Privacy
NO.:	ADMIN-222
RESPONSIBILITY:	Vice President, Corporate Services and Chief Financial Officer
APPROVED BY:	Durham College Leadership Team

1. Introduction

Durham College ("the College") is committed to protecting the privacy of students, employees, alumni, and community partners. We collect, use and disclose personal information in accordance with relevant privacy legislation. The primary legislation that governs the College's activities with respect to access and privacy is the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Protection Act (PHIPA).

2. Purpose

This policy communicates how the College collects, uses, discloses, safeguards and retains personal information and personal health information consistent with relevant legislation and regulations and outlines processes related to accessing records and reporting and responding to privacy breaches.

3. Definitions

Refer to DC's Standard Definitions.

4. Policy statements

4.1. Applicability

4.1.1.
This policy and procedure applies to all records in the College's custody and control, including administrative and operational records created as part of the day-to-day business operations, whether in paper or electronic format and may include but is not limited to communications such as emails, text messages, chatbot interactions, online meeting chats, or other digital content that contains personally identifiable or other confidential information.

4.1.2.
All employees, contractors, volunteers and third parties who process personal information or personal health information on behalf of the College are expected to follow the established procedures and protocols for data security, privacy, and record keeping.

4.2. Accountability and Governance

4.2.1. Under FIPPA, the Chair of the Board of Governors, as designated Head of the College, has the power and duty to make decisions on requests to access and correct College records. The Board Chair has delegated these powers and duties to an officer of the College, the Vice President, Corporate Services and Chief Financial Officer, who will act as the Freedom of Information (FOI) Coordinator. In turn, the Vice President, Corporate Services and Chief Financial Officer has delegated the role of FOI Coordinator to the Manager, Board Governance and Privacy but remains ultimately the senior executive accountable for the College's privacy program.

4.2.2. As FOI Coordinator, the Manager, Board Governance and Privacy will be the contact person for all public inquiries regarding access requests under FIPPA. This individual will review all requests for access and correction, and rule on refusals, exemptions, transfers, severance and third-party notifications.

4.2.3. With respect to the PHIPA, the Board has appointed the Manager, Board Governance and Privacy as the contact person for Durham College under Section 15(2) of the Act.

4.3. Collection and Use

4.3.1. The College collects personal information and personal health information in accordance with applicable privacy legislation and only for purposes that align with the College's mandate and objectives.

4.3.2. The College will endeavour to only collect the minimum amount of personal information or personal health information necessary to accomplish a function or to comply with a Ministry reporting requirement.

4.3.3. The primary purposes for which the College collects personal information from students, prospective students, employees, and alumni include but are not limited to the following:

- Activities related to academic and non-academic programs;
- Administering the alumni relations program;
- Employment-related matters;
- Experiential learning activities;
- Financial aid assistance, awards, and bursaries;
- Health and safety activities;

- International activities and global engagement;
- Institutional planning, research, and statistical reporting;
- Philanthropic initiatives and activities;
- Providing services such as peer tutoring, academic accommodations, career assistance;
- Recruitment, admission, registration and graduation;
- Information technology services;
- Supporting participation in various administrative activities (e.g., athletics, residence, food service, transit pass)
- Working with third-party organizations for COLLEGE-sponsored activities.

4.3.4. The College will only collect personal information directly from the individual to whom the information relates unless:

- The individual authorizes another manner of collection (e.g., from someone else);
- The information is collected for the purpose of determining suitability for an award;
- The information is collected for law enforcement purposes.

4.3.5. The College will only use personal information for the purpose it was collected or a consistent purpose, except where required or permitted by law or with the consent of the individual. The College will never sell personal information to any third party, organization or person for any reason without prior consent or notice.

4.3.6. Where the College collects personal information, it will inform individuals to whom the information relates via a Notice of Collection that includes:

- The legal authority for the collection;
- The primary purpose(s) for which the personal information is intended to be used; and,
- The title, business address, and business telephone number of the College official responsible for answering questions about the collection.

4.4. Consent

4.4.1. The College will obtain express or implied consent before collecting, using, or disclosing personal information, except where otherwise permitted or required by law.

4.5. Disclosure

4.5.1. The College may disclose personal information or personal health information to comply with a warrant or subpoena, or for the following reasons:

- To support legitimate purposes related to College activities (e.g., service providers contracted by the College, other post-secondary institutions to verify information);
- Where appropriate to relevant government ministries and entities and quality assurance agencies;
- In emergency or compassionate situations where there is a real risk of harm not to disclose. Where possible, the College will inform the individual of the disclosure where it is able to do so.
    - It is for this reason that employees and students are encouraged to keep current emergency contact information on file.

4.5.2. The College may disclose, outside of the formal access 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 list of students who obtained honour roll status on a semester basis;
- General program and course information;
- Information about a College employee in their professional capacity (e.g., name, title, College email address);
- Other documents that are publicly available on the College website;
- Permanent academic records forming part of the student record such as transcripts, letters of verification, official receipts, tuition tax forms, and duplicate credentials;
- Public agendas and minutes of the Durham College Board of Governors meetings and the Governance Review Committee

meetings;

- The College's annual report, business plan, and strategic vision;
- The College's executed strategic mandate agreement;
- The names and biographies of the College's Board of Governors;
- Verification of employment or employment records;
- Whether a student has received a credential conferred by the College and the date of conferral. The College publishes a list of graduates including the student's name, program, distinction, and term of graduation; and
- Whether a student has received a particular academic award, honour, or distinction from the College or an external third party.

4.6. Safeguarding of Personal Information

4.6.1. The College will take reasonable steps to protect personal information and personal health information against loss, theft or unauthorized access, disclosure, copying, use, or modification, regardless of the format in which the information is held, using appropriate controls. Controls may include, but are not limited to:

- Administrative controls (e.g., policies, training, separation of duties)
- Data Governance controls (e.g., framework for managing data throughout its lifecycle)
- Operational controls (e.g., incident response plans)
- Physical controls (e.g., locked cabinets, access cards, surveillance cameras)
- Technical controls (e.g., firewalls, multifactor authentication, access control)

4.6.2. Access to personal information or personal health information will be restricted to individuals, programs and offices that are legally and operationally authorized. The College is committed to applying the principle of least privilege, ensuring that users, systems, and processes are granted only the minimum level of access necessary to fulfill their designated responsibilities.

4.6.3. Before collecting personal information, the individual with oversight of the activity will complete a Privacy Impact Assessment to identify the actual or potential effects that a proposed or existing information system, technology, program, process or other activity may have on an individual's privacy.

4.6.4. If the College engages a vendor to process personal information on its behalf or wants to procure a new system, technology or tool, the College will conduct the necessary vendor due diligence and ensure the vendor can comply with the College's privacy and security obligations. This due diligence may include an information technology security assessment, other assessments, and the execution of contracts or agreements.

4.6.5. The College reserves the right to establish minimum information security standards for all systems, tools, or technologies.

4.7. Correction

4.7.1. The College will investigate and act on an individual's request to correct records that contain their personal information or personal health information, where appropriate.

4.8. Retention and Disposal

4.8.1. Personal information will be retained for one year from its last use unless it is required to be maintained for longer in accordance with the College's Common Records Retention Schedule.

4.8.2. The College will take reasonable steps to dispose of personal information and personal health information securely.

5. Access Procedures

5.1.1. Before making a formal request under FIPPA for access to personal or general records, individuals should contact the department or Faculty directly to determine if they can access the information, and/or to follow the standard process for the types of records being sought.

5.1.2. Individuals seeking to make a formal request under FIPPA or PHIPA should be directed to DC's How to Access Records webpage.

5.1.3. The College will process all formal requests made under FIPPA or PHIPA as prescribed by the legislation and according to the statutory timelines contained therein. Fees may apply.

5.2. Student Access to Their Own Personal Information

5.2.1. Students can access and review records about themselves held by the College, except student evaluations, documents about academic achievement at other institutions, and letters of reference supplied by the College. Most permanent academic records can be accessed or requested directly by the student through MyDC. Fees may apply.

5.2.2. Students must present valid government-issued photo identification or campus identification that includes a photo to view their records.

5.2.3. Students must access 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 must have supervised access to the record electronically when a physical record is not maintained.

5.2.4. Students may not remove records from their files.

5.3. Employee Access to Student Records

5.3.1. The extent of access to student records will correlate to the employee's job responsibilities, as described in the employee's job description and approved by their supervisor.

5.3.2. Access to student personal health information is limited to those employees providing relevant, direct support to the student.

5.3.3. An employee's supervisor may withdraw the employee's access to student records at any time.

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 Faculty or 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 the FOI Coordinator using the Third Party Request for Student Records form.

5.5. Access to Employment Records

5.5.1. The Human Resources and 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.

6. Privacy Breach Protocol

6.1. The College's privacy breach protocol applies to all personal information and personal health information held by the institution. If the personal information breached is related to personal health information, then the Manager, Board Governance and Privacy will work with the Director, Campus Health and Wellness Centre, or designate, to respond to the breach appropriately.

Step 1: Identification and Alert

6.2. 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:

a) Upon identifying a potential privacy breach, the employee, volunteer, agent, or contractor will notify a supervisor or manager, who will notify the Manager, Board Governance and Privacy in writing using the Privacy Breach Reporting Form found on ICE or by emailing privacy@durhamcollege.ca.

b) If a supervisor or manager is unavailable, the employee, volunteer, agent, or contractor will contact the Manager, Board Governance and Privacy to report the potential privacy breach.

c) The Manager, Board Governance and Privacy 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 the College and Ontario Tech University, the Manager, Board Governance and Privacy will notify the university as soon as practicable.

If it is determined that a privacy breach has occurred, the Manager, Board Governance and Privacy, in consultation with the Vice President, Corporate Services and Chief Financial Officer will implement steps 2 through 4 of the process and engage appropriate functional areas as required by the nature of the breach (e.g., IT security, Human Resources, Risk Management).

Step 2: Containment

6.3. The Manager, Board Governance and Privacy will, in consultation with the relevant Executive Leadership Team member:

6.3.1. If possible, retrieve and secure any records associated with the breach and retrieve copies of any personal information that has been disclosed;

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

6.3.3. Take steps, where able, to ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information, including determining if any copies were forwarded to another party;

6.3.4. 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

6.3.5. Take any other action necessary to contain the breach.

Step 3: Notification

6.4. The Manager, Board Governance and Privacy will, in consultation with the Vice President, Corporate Services and Chief Financial Officer:

6.4.1. Notify all members of the Executive Leadership Team.

6.4.2. Notify the Information and Privacy Commission (IPC):

a) The requirement to notify the IPC regarding a privacy breach is stated in PHIPA S.12 and FIPPA S. 40.1 (and as defined in regulation). To ensure compliance with relevant privacy laws, the College will notify the IPC when:

- The breach involves personal health information of one or more individuals (subject to PHIPA's Mandatory Reporting of Breaches); or
- The breach involves the theft, loss, or unauthorized use or disclosure of personal information that creates a Real Risk of Significant Harm to an individual. Factors that are used to determine if

there is a Real Risk of Significant Harm include:

i. The sensitivity of the information;

ii. The probability that the information has been, is being, or will be misused;

iii. The availability of the steps the individual could take to reduce or mitigate the risk;

iv. Directions, recommendations, or guidance provided by the IPC of what constitutes a Real Risk of Significant Harm; or

v. Other factors considered relevant by the Manager, Board Governance and Privacy.

6.4.3. Notify the individuals whose privacy was breached if there is a potential for a Real Risk of Significant Harm. The decision to notify individuals may be made in consultation with the Executive Leadership Team, legal counsel, the College's insurers, and/or the incident response partner. Notice may be completed by telephone, in person, or in writing and include:

- General information about the incident and its timing;
- A description of the personal information or personal health information involved;
- Information on how the College will assist individuals, and provide steps the individual can take to reduce the risk of harm and further protect themselves (if applicable);
- The contact information of the Manager, Board Governance and Privacy, and if required, the contact information of another individual at the College who can respond to department-level questions;
- Notice that the College has notified the IPC (if applicable); and,
- Notice that the individual is entitled to make a complaint to the IPC.

6.4.4. In the case of records pertaining to the Ontario Student Assistance Program, notify the Ministry of Colleges, Universities, Research Excellence and Security.

6.4.5. Notify law enforcement, if necessary and appropriate.

Step 4: Investigate and Conclude

6.5. The Manager, Board Governance and Privacy will in consultation with the appropriate parties:

6.5.1. 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;

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

6.5.3. Ensure employees, volunteers, agents, and contractors are appropriately educated and trained concerning privacy requirements.

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. Every person who is convicted under Section 61 of FIPPA is guilty of an offence and liable to a fine not to exceed $5,000.

8.2. Effective January 1, 2024, the IPC can issue administrative monetary penalties for non-compliance with PHIPA of up to $50,000 for individuals and $500,000 for organizations.

8.3. 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
- Third Party Request for Student Records Form