Access and Privacy Policy

Purpose/Rationale:

The Humber College Institute of Technology and Advanced Learning, and the University of Guelph-Humber (hereafter referred to as “Humber” or “the College”) is a public institution and is committed to ensuring compliance with existing legislated and regulatory responsibilities regarding information privacy and access, the adoption of high standards of information protection and sound record handling. The College commits to providing the public with access to records while also meeting legal obligations to protect the privacy of personal information under its custody or control. This policy ensures Humber’s practices support privacy protection consistent with *The Freedom of Information and Protection of Privacy Act* and other legislation that may apply.

This document is available in alternate format on request.

Scope:

This Policy applies to all employees and faculty of Humber, and the University of Guelph-Humber, all of whom are collectively referred to herein as “employees” as well as contractors, student workers and others who perform work for Humber; at all Humber campuses and specifically to records or information under Humber’s custody or control, including administrative and operational records created in the conduct of Humber day to day business operations. Particular care is to be taken with records which contain Personal or other Confidential Information.

Definitions:

Collection: means the act of gathering acquiring, recording, or obtaining Personal Information from any source and by any means.

Consent: means a voluntary agreement to a collection, use and/or disclosure of Personal Information for identified purposes.

Confidential Information: is information intended for limited distribution and not to be generally or publicly available, e.g. Human Resources records, personal health information, third party commercial information, solicitor client / legally privileged information, research or teaching materials, records in draft, development, un-approved or non-final state, non-public financial information, etc.

Control (of a record): means the power of authority to make a decision about the use or disclosure of the record.

Custody (of a record): means the keeping, care, preservation or security of the record for a legitimate business purpose. While physical possession of a record may not always constitute custody, it is the best evidence of custody.

Data Steward: means the individual as designated by an appropriate executive sponsor who is responsible for maintaining and protecting a defined set of data (i.e. enrollment records).

FIPPA: refers to the *Freedom of Information and Protection of Privacy Act (Ontario).*

Formal Access Request: refers to a request for access to information which cannot be answered through existing or established processes. A Formal Access Request is processed in compliance with the procedures outlined in FIPPA and requires the completion of a Request Form with sufficient details regarding the nature of the information being sought and a $5 application fee. Such requests are processed by the Office of Legal and Risk Management, may take time to process and may require payment of additional fees.

Informal Access Request: refers to a request for access to records that are readily available and appropriate for release without requiring a fee or Formal Access Request. Typically are appropriate when a review of exemptions or exclusions is not necessary and requests are received for the same information on a routine basis.

Personal Information: is defined in FIPPA and refers to recorded information about an identifiable individual, including but not limited to:

- information relating to the race, nationality or ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status of the individual
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved
- any identifying number (e.g. student number), symbol or other particular number assigned to the individual
- the home address, or e-mail address, telephone number, fingerprints or blood type of the individual,
- personal opinions of, or about, an individual except where they relate to another individual,
- correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence
- the views or opinions of another individual about the individual, and
- the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual

Business Identity Information: Information regarding individuals acting in their business, professional or official capacity such as name and title, contact information, work address (including office location), work telephone number, Humber employee e-mail address, etc. is not usually considered personal information.

Personal Health Information (PHI): is confidential recorded information about an identifiable individual related to the individual's health or the provision of treatment services to the individual, subject to PHIPA s. 4(1).

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

PHIPA: refers to the Personal Health Information Protection Act (Ontario).

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

- correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, including drafts; and
- any record that is capable of being produced from a machine readable record under the control of the institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution, or to which the institution can reasonably gain access;
- e-mail, text and mobile phone records, other social media or application information used for business purposes, including additional/forwarded copies.

Designated Official: refers to the office of the individual who has authority to act in administrative capacity at Humber and responsible for developing, maintaining, review, administering and implementation of the policy or procedures under the direction of an Executive member.

Student: refers to any individual who is, or has been, admitted, enrolled, or registered for study at Humber. Individuals who are active in a program, but not enrolled in classes for a particular term (e.g. vacation or leave) are considered to have a continuing student relationship.

Third Party: refers to a person, group of persons, or organization other than the individual the information is regarding. Employees and faculty members of Humber, acting in an official capacity, are not considered third parties.

Policy:

1. The College is responsible for the information in its custody or control and will comply with applicable privacy legislation in dealing with such information. Humber will create information handling practices that reflect the College's commitment to the protection of personal privacy and data security and will actively monitor and review those practices to ensure that they are reasonable and reflect current best practices. FIPPA creates a public right to request records from the College. FIPPA protects individual privacy by regulating College actions involving Personal Information, including how it is collected, used and disclosed. College employees are responsible for reviewing and understanding the Policy and related Procedures.

2. Collection, Use and Disclosure of Personal Information

   2.1. No person shall collect personal information on behalf of the College unless the collection is expressly authorized by statute; necessary for the proper administration of a lawfully authorized activity; and is necessary for established College functions, operations essential to the College's educational mandate and activities; and in accordance with Humber's legitimate business purposes. When collecting information, the College will endeavor to only collect the minimum amount of Personal Information

necessary to accomplish the function.

2.2. The College must have legal authority to collect information, meaning:
- 2.2.1. Collection must be expressly authorized by statute (e.g. certain sections of the *Labour Relations Act, Occupational Health and Safety Act, Statistics Act*, MTCU Act etc.).
- 2.2.2. The information is to be used for purposes of law enforcement, or
- 2.2.3. Collection is necessary for established College functions in accordance with applicable laws, or
- 2.2.4. Collection is necessary for the proper administration of a lawfully authorized activity or as otherwise authorized by FIPPA.

2.3. Personal Information shall be collected directly from the individual to whom the information pertains unless:
- 2.3.1. The individual authorizes another manner of collection (i.e. from someone else),
- 2.3.2. The information is collected for the purpose of determining suitability for an honourary award,
- 2.3.3. The information is collected for purposes of law enforcement.

    2.3.3.1. The College has legal obligations of due diligence to ensure all employees and students have the right to work and study in a safe environment, including cooperating with requests from the police when they suspect that a person of interest may be associated with Humber. FIPPA permits the disclosure of Personal Information to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result (section 42 (g) of the *Act*). Any requests by police for information regarding students or employees are to be directed to the Chief Privacy Officer to determine what Personal Information can be released and to maintain a record of the request.

2.4. A Notice of Collection is required when collecting Personal Information, including:
- *2.4.1.* The legal authority for the collection of the information,
- *2.4.2.* The principal purpose(s) for which the information is intended to be used,
- *2.4.3.* Title, business address and phone number of a College official to answer questions about the collection
- *2.4.4.* All forms/documents by which Personal Information is collected shall indicate the same information.

2.5. Personal Information shall be used only for the purpose for which it was collected or a consistent purpose, except where required or permitted by law or with the consent of the individual. A purpose is consistent if the use is “reasonably compatible” with a purpose given on collection or in a Notice of Collection as defined in the *Act*. When used for a purpose not previously identified, the new purpose shall be identified and the consent of the individual shall be required prior to use. Humber will not sell or rent Personal Information to any third party organization or person for any reason without prior consent or prior notice.

2.6. The availability of Personal and other Confidential Information is to be limited to legally and operationally entitled individuals, programs and offices. A request by a Humber staff member or team for access to Personal Information of a Student or staff member

should be directed to the most responsible Data Steward with consultation from the Chief Privacy Officer as required. Access will be provided only if the Humber official needs the information in order to do his/her job.

2.7. Students and other individuals have a right of access to Personal Information about themselves in the custody or control of Humber subject to specific and limited exceptions as outlined in FIPPA. A request by a Student or other individual for access to his/her own Personal Information should initially be directed to the most responsible office (e.g. Faculty Dean or designate), that holds the Personal Information, or by following existing procedures for access. If there is no process in place, the applicant may file a Formal Access Request with the Office of Legal and Risk Management. A Formal Access Request must be made in writing and must be accompanied by the Request Form and a $5.00 application fee (https://humber.ca/legal-and-risk-management/foi.html).

2.8. Personal Information shall not be disclosed except in limited circumstances such as:

2.8.1. With the prior consent of the individual to whom the information pertains;
2.8.2. Disclosure for purpose(s) for which the personal information was collected;
2.8.3. Need to know; to a Humber employee, officer, agent or contractor who needs the information to perform official, proper College duties (i.e. who require the record for performance of their duties);
2.8.4. Externally ONLY as required by law, established in College policy;
2.8.5. In compelling circumstances affecting the imminent health or safety or an individual(s);
2.8.6. In compassionate circumstances to facilitate contact with a spouse, close relative or friend of an individual who is injured, ill or deceased.

2.9. Personal Information of a Student or employee shall not be disclosed to a third party except:

2.9.1. With the prior consent of the individual;
2.9.2. To a law enforcement agency in Canada to aid in an active investigation;
2.9.3. In compelling circumstances affecting the health or safety of an individual; or
2.9.4. For College related fundraising activities pursuant to Section 41(2) or
2.9.5. Otherwise, in accordance with FIPPA.

2.10. The Office of Legal and Risk Management will establish, maintain and be responsible for the process for responding to Formal Access Requests.

2.11. Personal Information shall only be kept for one year after its last use unless the person to whom it pertains consents to earlier disposal or as long as necessary to satisfy the purpose for which it was collected in accordance with the College's Record Retention Schedule. College record retention or legal requirements may necessitate that the information be kept longer as per Humber's Record Retention Schedule.

2.12. The College will strive to provide users with the ability to update their own Personal Information where possible.

3. FIPPA Exemptions

Some records are exempted from disclosure and must not (mandatory) or may not be released under FIPPA. Consult the Office of Legal and Risk Management in such situations.

4. Security

4.1 Humber will take all reasonable measures to ensure that Personal Information collected is accurate, complete and current. Privacy is an overarching institutional responsibility shared by all members of the College. College employees are required to prevent unauthorized access to records and to implement security measures to ensure the orderly and efficient creation, use, maintenance, retention and disposal of records according to legal, fiscal and statutory requirements, and administrative or operational needs. College employees should protect Personal and Confidential Information from unauthorized access and unintended destruction (e.g. locked filing cabinets, password protection, fully encrypted laptops and USB memory sticks).

4.2 Privacy and confidentiality must be supported with strong security; technical, physical and administrative measures that protect information through its lifecycle, from creation or collection to disposal. Electronic or hard copy records that contain Personal and other Confidential Information shall not be removed from a secure institutional environment unless they can be kept secure, with official authorization from the appropriate Data Steward, operational need and no other reasonable means to complete the task. The College takes all reasonable measures to protect Personal Information and systems used to store Personal Information. This includes maintaining organization processes and capabilities to limit access to Personal Information to only those individuals who require access to it to fulfill the purpose for which it was collected.

4.3 While each Department/Faculty creates, receives, uses and maintains records that relate to the administration or operation of the College, these records are and remain the property of Humber.

4.4 In some Departments/Faculties, employees with access to Personal and/or Business Information in the custody or control of the College may be required to agree in writing to respect the confidentiality of the Personal and/or Business Information to which they have access.

4.5 Security measures to be considered include compliance with the College *Acceptable Use Policy/IT Security Policy (embed link to policy),* Humber's *Third Party Service Provider Security Standards* (embed link to these standards) and the following:

- computer use procedures (e.g. password restrictions, shutting off computers while not in use, encrypting files with Personal Information, not transporting Personal Information on USB, not emailing Personal Information etc.);
- firewalls;
- physical security (e.g. locking cabinets and offices); and,
- administrative protocols (e.g. limiting staff access to certain files; use of shared electronic files, etc.).

5. Retention & Disposal

5.1 Personal Information shall be retained for one year from its last use unless it is required to be maintained for a longer period in accordance with the College Retention Schedule.

5.2 Humber employees shall take reasonable steps to protect the security and confidentiality of Personal Information during its collection, storage, handling and destruction.

5.3 When information is destroyed, Humber employees shall take reasonable steps to ensure information cannot be reconstructed or retrieved, documenting record destruction and retaining for future reference.

6. Privacy Breach Event Incident Response

Immediately report all actual or potential privacy incidents, such as inappropriate disclosure of personal information to your supervisor and the Chief Privacy Officer. The Chief Privacy Officer will guide the incident response in coordination with other internal and external stakeholders as appropriate and provides support to ensure a quick and effective response that meets legal requirements.

7. Accountability

7.1 Humber's designated official with responsibility for ensuring compliance with the provisions of FIPPA and PHIPA is the Associate Vice President, Legal and Risk Management.
7.2 The Associate Vice President, Legal and Risk Management may delegate parts of her/his responsibility to others as appropriate.
7.3 The Associate Vice President, Legal and Risk Management will:
   a. Coordinate the development and implementation of policies, procedures, practices and/or guidelines to manage compliance with FIPPA; and
   b. Provide support services to Humber employees on matters pertaining to the protection of Personal Information.

8. Records Management

Records are considered an institutional asset and therefore must be managed to maximize their usefulness to College operations. Data Stewards for various data sets in consultation with the Chief Privacy Officer are responsible for ensuring that Records are properly protected and maintained and also appropriately utilized across the College. Humber staff should:

- only create records as necessary to conduct College business;
- preserve official records needed for College business or to document actions taken;
- follow the College Records Retention Schedule; and
- delete transitory records, such as rough notes, drafts, copies and personal messages.

9. Recording Meetings

Meeting records should only capture information needed to achieve meeting objectives. Establish meeting record parameters and how Personal or Confidential Information shall be protected. Avoid creation of unofficial meeting records. See FIPPA Tip Sheet – Best Practices

10. Questions or Complaints

The Office of Legal and Risk Management will respond to questions or concerns regarding Humber's management or treatment of Personal Information.

11. Authority

The Responsible Office for this Policy is the Office of Legal and Risk Management.

References:

Acceptable Use Policy
Freedom of Information and Protection of Privacy Act (Ontario)
Personal Health Information Protection Act (Ontario)

Appendices:

Appendix A: FIPPA Request Form

Related Policies:

Acceptable Use Policy
IT Security Policy
Information Governance Policy

Related Procedures:

Records Retention Schedule
Record Destruction Form
Privacy Impact Assessment
FIPPA Tip Sheet – Best Practices
Privacy Breach Procedure