Data Governance 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 data. Institutional data are an important and strategic asset of Humber College that directly support the institution’s mission and mandate. These data are used to inform College operational functions as well as guide policy formation, program development, assessment and strategic planning. The utility of these data is derived from its quality, integrity, security, and ease of access. As such, sound data governance and management are essential to the attainment of institutional goals.

The purpose of this Policy is to:

- Establish clearly defined roles and responsibilities with corresponding accountability for effective and transparent management of institutional data assets.
- Institute best practices for robust data management aimed at enhancing data quality and integration, mitigating data security risks and privacy concerns, increasing data accessibility and utilization, and improving data definitions and metadata.
- Foster a culture of skillful and responsible data use as an integral part of institutional management and planning.

This document is available in alternate format on request.

Scope:

This Policy applies to all users of Institutional Data regardless of the data’s location of access (on campus or off campus), affiliation (internal or external to Humber), medium of data delivery (e.g., electronic, paper, audio-visual), form of data storage (internal or external server), mode of data (system view or extraction) and the level of data transformation (raw, revised or derived).

Definitions:

Institutional Data: Institutional Data is defined as those data elements or holdings created, collected, maintained, recorded or managed by Humber College that are relevant to the operations, planning or management of any department or unit or, are data that are reported or used in official administrative institutional reports.

Executive Sponsors: Executive Sponsors are senior college officials who have planning and policy responsibility and accountability for major administrative data systems (e.g., student, human resource, financial) within their functional areas.

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). Data Stewards are responsible for safeguarding data from unauthorized access through established

procedures and educational programs. They authorize the use of data within their functional areas and monitor this use to verify appropriate data access. They support access by providing appropriate documentation and training to support college data users.

Data Administrators: Data administrators are college employees who usually report to a data steward and whose duties provide them with an intricate understanding of the data in their area. They work with the Data Stewards to establish procedures for the responsible management of the data including data entry and reporting. Some Data Administrators may work in an information and technology department outside of a functional unit but have responsibilities for implementing the decisions of the data stewards. Technical Data Administrators may be responsible for implementing backup and retention plans or ensuring the proper performance of database software and hardware.

Data Users: Data Users are individuals who make use of Institutional Data while performing assigned duties or fulfilling their authorized role within the College. Although Data Users are typically full time, permanent employees (e.g., faculty, administrators, support staff), other employees such as contract, consultants, agents, students, volunteers and guests who have demonstrated a legitimate need for the data to carry out their approved function at Humber College may become a data user for the duration of their work or affiliation.

Data Governance Structure: In the interest of ensuring effective data governance, Humber College applies formal guidelines to manage the institution's information assets and assigns personnel to implement them. These responsibilities are shared among the executive sponsors, Data Stewards, Data Administrators and Data Users.

Data Access: It is the intent of Humber College to promote a culture of collaboration, transparency and data-driven decision-making. Consistent with this approach, the College, as the data owner, intends for its institutional data to be readily available to all authorized members who demonstrate a legitimate business need for the information, subject to any limitations that may be posed by federal or provincial regulations.

Policy:

1. Data Security

    1.1. Institutional Data must be secured and protected to comply with federal and provincial regulations and to ensure their integrity and availability to members in the Humber College community. Failure to maintain data security may not only result in the corruption, loss or devaluation of important data but may also result in legal repercussions, financial penalties and the ability to the institution to meet its mission. Everyone at Humber College must commit to safeguard Institutional Data against misuse or abuse. At the same time, it is important for data security procedures and guidelines to maintain an appropriate balance between security and accessibility and to be consistent with Humber's IT Security Policy.

2. Classification of Institutional Data

    2.1. The foundation for data security at Humber College is based on data classifications and

a framework for handling institutional data based on its criticality and sensitivity. Data Stewards implement security controls in accordance with the data's assigned classification level and any other applicable laws or regulations.

2.2. The classification system is based on proprietary, strategic, legal and ethical considerations. Higher levels of criticality or sensitivity require stricter security controls. Humber's institutional data covered by this policy are assigned to one of three categories in order of most critical/sensitive to least.

	Restricted Data	Sensitive Data	Public Data
Institutional Impact	The negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is usually very high and may include legal, financial, and reputational consequences.	The negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is moderate to high.	Public data does not pose a risk in terms of confidentiality but its quality and integrity is important to the reputation of the institution.
Description	Access to restricted data must be controlled from creation to destruction and is granted only to those affiliated with the college who require the data to perform their job. Included in restricted data are those which fall under privacy legislation including FIPPA and PHIPA. Also included are data related to highly sensitive College business including that may be legal, proprietary and strategic.	Sensitive data are intended to be protected from broad consumption on account of business concerns, such as those related to competition and institutional strategic decision-making. Examples may include data related to budgeting, financial reports, facilities and human resource information.	Public data is typically highly aggregated data such as those reporting high level college enrolments and other publically reported metrics.
Access	Access to these data occur only when it is in accordance with Humber's legitimate business purposes and when legislation permits. Requests for access should be directed to the Executive Sponsor or relevant Data Steward.	Access to these institutional data may be authorized by the Data Steward to groups or individuals based on their job classification or role. Authorized personnel may be given access to systems but typically to subsections of the data (e.g., as reports or dashboards) to prevent access to more sensitive	Access to these data may be granted to any requester and will typically be through public websites or through requests to Data Stewards or Data Administrators in specific departments, such as Institutional Planning and Analysis or through the

		data that is not required for business purposes.	Communications departments.

3. Executive Sponsors

3.1. Executive Sponsors may include the following administrative personnel currently in place at Humber College: Senior Vice President, Transformation and Strategic Partnerships; Senior Vice President, Academic; Vice President, Human Resources and Organizational Effectiveness; Vice President Administration and CFO; Vice President, Students and Integrated Planning; and Chief Information Officer.

3.2. Specific responsibilities include:

- Establish and refine the Data Governance Policy.
- Provide overall strategic direction for the data governance program.
- Hold final authority over institutional data in their operational divisions.
- Evaluate the progress and initiatives of the data governance program annually.
- Promote a culture of data-driven decision-making.
- Arbitrate on issues of contention surrounding Institutional Data including denial of access to data and violations of Data Governance Policy and address issues identified by the Data Stewards.
- Identify Data Stewards responsible for each data element in their purview.

4. Data Stewards

4.1. Included among Data Stewards are the following administrative personnel: Associate Director, Institutional Research; Associate Registrar, Student Systems and Reporting; Associate Director, Financial Planning; Director, Advancement Services; Director, HR Support Services; Associate Director, Campus and Space Planning.

4.2. Specific responsibilities include:

- Implement procedures to provide proper access to Institutional Data in their purview, maintain the quality of those data and safeguard the data from unauthorized access and misuse.
- Classify the data under their purview according to its sensitivity to direct access to and disclosure of that meets security purposes.
- Understand institutional business needs and facilitate appropriate access to data by setting clear guidelines for access to and review of Institutional Data.
- Investigate reports of data inaccuracies and initiate remediation as appropriate.
- Promote consistent data interpretation and usage, prevent data loss and misuse, and enhance reporting capacity to support institutional data-driven decision-making.
- Ensure data systems are protected from corruption and establish data backup and recovery procedures.
- Ensure appropriate logical integrity in the databases.
- Establish data collection standards and mechanisms for data validation, data synchronization and error detection to ensure the accuracy of institutional data.
- Establish interfaces to connect information systems in different functional areas, develop synchronization mechanisms, assimilate key data elements and minimize

duplication or redundancy of data.
- Ensure data is available in a timely manner and on expected schedules.
- Provide adequate training and documentation to support data users including data definitions in the College data dictionary.

4.3. Collectively, the Data Stewards form the Data Management Group (DMG). The role of the DMG is to guide and support the institution in the development, maintenance and continuous improvement of its integrated institutional data holdings. Key responsibilities include:
- Establish guidelines, policies and processes to ensure appropriate access to Institutional Data, maintain the quality and integrity of those data and safeguard the data from inappropriate access and misuse.
- Facilitate cross-functional access and use of Institutional Data through discussion and collaboration on data coordination, data definitions and glossaries, and data stewardship, informed by the advice of institutional resources responsible for data security, access, and protection of privacy.
- Support the education of Humber personnel in the appropriate use of Institutional Data.

4.4. In addition to the Data Stewards, the DMG may include other key decision-makers who play a role is the management of the College's data assets including:
- Director, Information Technology, Security and Project Management.

5. Data Users

5.1. All individuals who have access to institutional data have an obligation to engage in responsible, proficient and scrupulous use of those data. They must access and use the data only in the conduct of official college business to which they have been assigned and in a manner that advances the institutions mission.

5.2. Responsibilities of the Data Users include:
- Follow the requirements for data security, protect their access credentials, maintain confidentiality of data and accurately present Institutional Data.
- Consult the applicable Data Steward when clarification is needed on the appropriate use and release of Institutional Data.
- Immediately report concerns regarding the compromise of data security (e.g., unauthorized access, disclosure, loss, etc), data errors, missing data or other data quality concerns.

5.3. Each Data User is accountable for the consequences of misuse or abuse. Those who fail to comply with institutional data policies, information technology policies, and/or related federal or provincial regulations may be subject to disciplinary action and other penalties.

6. Data Access

6.1. Individuals or departments may not deny access to Institutional Data under their control of the basis of proprietary rights. For the advancement of the College, Institutional Data must be securely shared among eligible campus members whose work can be

improved as a result of data availability, irrespective of whether these individuals belong to the department that collects or maintains the data, unless such sharing of data is restricted by provincial or federal regulations.

6.2. Authorization for access to data is not transferrable from one individual to another. Authorization is granted through the appropriate Data Stewards or other processes as outlined in this Policy.

6.3 Persons in need of access to Institutional Data must make a request through the e-form entitled Request a Report or Data Set. Review of data requests must be provided in a timely manner and the decision with rationale communicated to the requester in writing. An employee or non-employee may appeal denied access first through the Data Management Group and if dissatisfied may submit a final appeal to the Executive Sponsor. When appropriate, data files will be provided in lieu of access to data systems. This may occur when access to systems may result in access to data which is not in the conduct of official College business or when FIPPA regulations apply.

7. Violations of Data Governance Policy

7.1. Any Data User who violates Humber's policies related to data privacy, security, access and governance and/or federal or provincial regulations, may have their data access terminated.

References:

Freedom of Information and Protection of Privacy Act (Ontario) (FIPPA)

Personal Health Information Protection Act (Ontario) (PHIPA)

Related Policies:

Acceptable Use Policy
IT Security Policy
Access and Privacy Policy

Related Procedures:

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