Durham College Policy and Procedure

TYPE:	Administrative
TITLE:	Student Data Governance
NO.:	ADMIN-279
RESPONSIBILITY:	Vice-president, Academic and Vice-president, Student Affairs
APPROVED BY:	Durham College Leadership Team
EFFECTIVE DATE:	June 2020
REVISED DATE(S):	
REVIEW DATE:	June 2023

1. Introduction

Student Data is a Durham College (DC) asset and needs to be managed responsibly. The value of data as an asset is diminished by misuse, misinterpretation, alteration, or unnecessary barriers to access. Effective Student Data Governance leverages the value of this asset and leads to responsible and consistent practices and evidenced-informed decision-making.

2. Purpose

The purpose of this policy and procedure is to provide guiding principles and directives for the availability, use, integrity, and quality of Student Data at Durham College.

3. Definitions

Refer to Durham College's Standard Definitions.

4. Policy statements

4.1. This policy applies to all Student Data within the custody and control of the College, where the data is:

- In electronic form or in hard copy,
- Centrally located in administrative systems, or offices, or
- In raw form or is derived, summarized or aggregated.

4.2. Student Data should be classified as follows:

4.2.1. **Public Student Data (low level of sensitivity):** This is aggregate data that is not proprietary and that can be freely shared without concern for privacy breaches or ethical considerations. Access may be granted to any requestor. Example: College statistics and reports that appear in publications and on the DC website.

4.2.2. **Internal Student Data (moderate level of sensitivity):** applies to aggregate data protected due to proprietary, competitive, ethical, privacy considerations, even though there may not be direct implications on a legislative or regulatory basis. Internal data is restricted to employees designated by the College that have a legitimate business purpose for accessing such data. Examples: KPI analysis, enrolment projections, program review data and new program considerations.

4.2.3. **Restricted Student Data (high level of sensitivity):** applies to data protected by legislation, regulation or policy. This level also represents Information that isn't protected by legislation or regulations, but for which the Information Owner has exercised their right to restrict access. Examples: Personally Identifiable Information, Social Insurance Numbers (SIN), Salary Data, Financial Aid Data.

4.3. Student Data may be available to DC employees who need it in order to carry out their responsibilities. This availability will be balanced with the need to protect internal and restricted Student Data. The principle of availability acknowledges the use of multiple Information systems in the collection and management of Student Data, and the important connection between systems governance and Student Data governance.

4.4. Student Data shall be used to support the pursuit of legitimate academic, research, and administrative activities. Access to Student Data shall be governed by controls that minimize risk to an acceptable level.

4.5. Quality standards for Student Data shall be defined and monitored to ensure trust and confidence. Recognizing the importance of quality data for accurate reporting and evidence-based decision making, a common vocabulary and approved data definitions will be shared. Resolution of issues related to quality of Student Data will follow a consistent process.

4.6. Each Information Owner shall designate one or more Student Data Stewards, who will be responsible for the development and implementation of data management plans that address quality, availability, and accessibility of data. Student Data Stewards shall support the day-to-day management of the Information Owner's asset, ensuring the quality and integrity of Student Data that is provided to internal and external stakeholders. Student Data Stewards will be held accountable to their roles and responsibilities with regard to the management and protection of Student Data.

4.7. The Student Data Governance Committee has been established with a Terms of Reference and comprised of representatives from stakeholder groups across the college, who are charged with oversight and implementation of these policy statements. This committee will be chaired by the Dean of Research Services and the Director of Reporting & Student Systems.

5. Procedure

5.1. Public Student Data

5.1.1. Public Student Data will be made available on the Durham College website - Open Data Page.

5.2. Internal Student Data & Restricted Student Data Requests

5.2.1. All internal requests shall be sent to the respective Data Steward. If the Data Steward requires guidance on the implications on the privacy of the data requested, the Data Steward shall consult with the Freedom of Information and Protection of Privacy Coordinator. If the Data Steward requires guidance on the appropriateness of the data request, the Data Steward shall consult with the Chief Data Steward or designate and with relevant information owners where necessary.

5.2.2. All external requests shall be sent to the Freedom of Information and Protection of Privacy Coordinator by submitting the Student Data Request Form, which is located on the DC website.

5.2.3. The Freedom of Information and Protection of Privacy Coordinator will work with the external requestor to identify the scope of the request and the intended use of the Student Data. The Freedom of Information and Protection of Privacy Coordinator will forward the request and relevant details to the respective Data Steward. If the Freedom of Information and Protection of Privacy Coordinator or the Data Steward requires guidance on the appropriateness of the data request, they shall consult with the Chief Data Steward or designate and with relevant information owners where necessary.

5.2.4. The Data Steward will prepare information for both internal and external requestors and provide the reports to the Chief Data Steward or designate for approval before releasing the information. The Data Steward will respond to all internal requests and the Freedom of Information and Protection of Privacy Coordinator will respond to all external requests.

5.2.5. Based on strategic and operational priorities all parties will endeavour to respond to requests for Student Data as soon as practicable but in no case to exceed 30 business days.

5.2.6. If a request for Student Data is denied, the Data Steward will provide a rationale to the requestor. The requestor may appeal the denial by contacting the Information Owner within five business days.

6. Roles and responsibilities

6.1. The Durham College Leadership Team is responsible for reviewing and approving the policies and procedures required for Student Data Governance.

6.2. The Student Data Governance Committee is responsible for providing oversight and direction on a college-wide approach to Student Data Governance and management, aligned with research, policy, operational, and business needs. The Student Data Governance Committee may establish additional sub-committees and/or working groups to help complete its work.

6.3. As the College's Information Custodian for key services, Information Technology Services (ITS), in collaboration with Information Owners, are responsible for implementing safeguards to manage Student Data and access decisions regarding the collection, transformation, and use of Student Data that is contained within the systems for which ITS is responsible.

6.4. ITS will work with the Records Manager to manage classification, use, retention and disposal of Student Data.

6.5. Information Owners are responsible for ensuring that Student Data Governance policies and procedures are adhered to.

6.6. Communications and Marketing is responsible for posting selected public Student Data on the DC Open Data webpage and ensuring that the most current version is posted.

6.7. The Office of Research Services, Innovation and Entrepreneurship is responsible for producing the reports for publication on the DC Open Data webpage.

6.8. The Data Steward is responsible for receiving internal requests for internal and restricted Student Data, and coordinating responses.

6.9. The Chief Data Steward is responsible for identifying, training, and supporting Student Data Stewards in the effective performance of their duties, and approving responses to requests for Student Data.

6.10. The Freedom of Information and Protection of Privacy Coordinator is responsible for receiving external requests for internal and restricted Student Data, and coordinating responses.

6.11. Safeguarding of Student Data is a responsibility shared by all employees, beginning with the employee or office that creates or collects the data, and it is the continuing responsibility of all employees who subsequently access and use it. All employees are responsible for ensuring they are compliant with data governance procedures and standards.

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

Non-compliance could affect the College's ability to conduct business, respond to requests for Information, be transparent and accountable, and ensure confidentiality and privacy of personal Information. This would be a risk to the College both financially and to our reputation in the community.

9. Communications plan

- A message will be posted on ICE alerting employees when new or revised policies and procedures are added to ICE.
- Ongoing training sessions will be conducted to ensure updates and procedural changes are communicated to appropriate employees.

10. Related forms, legislation or external resources

- Freedom of Information and Protection of Privacy Act (FIPPA)
- Personal Health Information Protection of Privacy Act (PHIPA)