CÉGEP Heritage COLLEGE

51

CÉGEP HERITAGE COLLEGE
POLICY #51

CONCERNING
DATA CLASSFICATION AND HANDLING

COMING INTO FORCE: **September 17, 2025**

REVISED: **N/A**

ADMINISTRATOR: **Director of Information Systems and Technology**

Preamble[1, 2, 3]

The purpose of the present Policy is to define the principles, responsibilities, and rules for classifying and handling information at CÉGEP Heritage College (hereinafter referred to as the "College"). It supports the College's obligations under Quebec law and provides a framework for the protection of the confidentiality, integrity, and availability of institutional data throughout its lifecycle—from creation and use to storage and final disposal.

This policy is established in accordance with:

- *Act respecting the governance and management of the information resources of public bodies and government enterprises (CQLR, c. G-1.03),*
- *Archives Act (CQLR, c A-21.1)*,
- *Act respecting Access to documents held by public bodies and the Protection of personal information* (CQLR, c. A-2.1), and
- *Order number 2024-05 of the Minister of Cybersecurity and Digital Affairs dated December 12, 2024, concerning the Government Digital Data Security Classification Model.*

ARTICLE 1
Purpose

The present Policy aims to ensure the proper classification and secure handling of data at the College by establishing a unified framework that promotes responsible information stewardship. It ensures compliance with legislative and regulatory obligations, protects institutional data throughout its lifecycle, and assigns clear roles and responsibilities to mitigate legal, financial, and operational risks to the College and its stakeholders.

ARTICLE 2
Application

The present Policy applies to all data collected, stored, processed, accessed, or transmitted by the College in any format (physical or digital), across all departments, systems, and platforms. It applies to all personnel including employees, faculty, administrators, students, contractors, interns, and third-party service providers, who interact with institutional data.

ARTICLE 3
General Provisions

All institutional data must be classified before being stored, shared, or processed, and any unclassified data must be treated as Confidential by default. Access must follow the principle of least privilege and be reviewed quarterly. Vendors and third parties must sign agreements and comply with classification and protection requirements. Any suspected data incident must be reported to IT Services immediately. New systems or changes to existing ones must include classification assessments, and exceptions to the policy require formal approval from senior management. The College may audit data practices and mandate training for all staff annually.

ARTICLE 4
Data Classification

All institutional data must be classified according to its level of sensitivity and the potential impact that unauthorized access, modification, loss, or disclosure could have on the College's operations, reputation, legal obligations, or

[1] In the event of any conflict of interpretation between the French and English versions, the English version shall prevail.

[2] In the present document, the use of gender-neutral language is used solely for the purpose of simplifying the text and by no means is intended as discriminatory.

[3] See the Glossary for explanations of frequently used terms.

individuals' privacy. This classification framework enables appropriate handling and protection of data throughout its lifecycle. The classification levels are defined as shown in the table below.

Classification	*Sensitivity Level*	*Description*	*Examples (not exhaustive)*
Restricted	Very High	Data requiring the highest protection. Unauthorized disclosure may cause severe legal, reputational, or operational harm.	SIN, medical records, disciplinary files, credentials, background check results, banking information
Confidential	High	Sensitive data intended for limited internal use. Unauthorized disclosure could result in significant harm.	Academic records (grades and transcripts), HR files (performance reviews, contracts), financial statements, salaries and benefits, network diagrams and system configurations, exam/test banks
Internal	Moderate	Business data not intended for public release. Disclosure poses limited risk.	Internal emails, meeting minutes, policy drafts, department budgets, procedures, employee id
Public	Low	Approved for public distribution. No anticipated risk from disclosure.	Website content, policies, public report, job postings, press releases, course outline

ARTICLE 5
Data Handling Requirements

To ensure the protection of the College's data throughout its lifecycle, all data must be handled in accordance with its classification level. This includes applying appropriate access controls, secure storage methods, encryption standards for transmission, and approved disposal procedures. Each classification category requires distinct safeguards to mitigate risks related to unauthorized access, data breaches, or loss. The table below outlines the minimum data handling requirements for each classification level.

Classification	*Access Control*	*Storage*	*Transmission*	*Disposal*
Public	Unrestricted	Public websites or shared drives	No encryption required	Regular disposal
Internal	Role-based access	Internal College systems	Internal email or secure channels	Secure delete or shred
Confidential	Limited to authorized users	Encrypted and access-controlled systems	Encrypted email or secure file transfer	Digital wipe or certified destruction
Restricted	Strictly controlled and logged	Encrypted, segmented environments	End-to-end encrypted, with logging	Physical shredding or certified digital destruction

ARTICLE 6
Data Roles and Responsibilities

6.1 Roles Definitions

- **Data Owner**: The person within the organization responsible for managing, securing, and granting access to a specific dataset.
- **Data Controller**: The entity that decides why and how personal data is collected, used and is legally responsible for its protection.
- **Data Steward**: The person who ensures data is accurate, consistent, and properly managed on a day-to-day basis.
- **Data Custodian**: The IT team responsible for storing, protecting, and backing up the data. They manage the technical environment.
- **Data User**: Anyone who accesses and uses the data for their work or analysis, following the rules set by the data owner.

6.2 Roles Matrix by Data Type

Data Type	*Controller*	*Steward*	*Custodian*
Student Records	Academic Dean Director – Student Services	Registrar Associate Academic Dean Student Services Coordinator	Information Systems and Technology
Academic Data	Academic Dean	Associate Academic Dean Registrar	Information Systems and Technology
Employee Records	Director – Human Resources	Coordinator - Human Resources	Information Systems and Technology
Employee Contracts	Director – Human Resources	Coordinator - Human Resources	Information Systems and Technology
Payroll Data	Director – Human Resources	Coordinator - Human Resources	Information Systems and Technology
Procurement Records	Director – Procurement and Financial Services	Coordinator - Procurement and Financial Services	Information Systems and Technology
Financial Records	Director – Procurement and Financial Services	Coordinator - Procurement and Financial Services	Information Systems and Technology
IST Infrastructure Data	Director – Information Systems and Technology	Coordinator - Information Systems and Technology	Information Systems and Technology
Building Access Logs	Director – Building Services	Coordinator - Building Services	Information Systems and Technology
Camera Footage	Director – Building Services	Coordinator - Building Services	Information Systems and Technology
Marketing & Communications	Director General	Secretary General and Head of Corporate Affairs	Information Systems and Technology
Faculty Records	Academic Dean	Associate Academic Dean	Information Systems and Technology

Note: The overall ownership of the College's data rests under the authority of the **Director General**.

ARTICLE 7
Data Handling Through Lifecycle

To ensure the responsible management of institutional data, it is essential to apply appropriate controls at every stage of the data lifecycle, from collection to destruction. Each stage carries specific risks and responsibilities, requiring coordination between data owners, custodians, users, and stewards. The following table outlines the key actions and responsible parties for safeguarding data throughout its lifecycle.

Lifecycle Stage	*Key Actions*	*Responsible Party*
Creation / Collection	Collect data lawfully and with consent where applicable. Minimize sensitive data.	Data Owner / Data Controller Data Steward
Use / Access	Restrict access to authorized users. Apply least privilege principle.	Data Owner / Data Controller Data User Data Custodian
Storage	Store data securely, apply encryption and access controls as needed.	Data Custodian
Transmission / Sharing	Use secure/encrypted channels for Confidential or Restricted data.	Data Custodian Data User
Retention / Archiving	Retain data per retention policies; archive securely.	Data Owner / Data Controller Data Custodian
Disposal / Destruction	Dispose data using secure, approved methods; prevent recovery.	Data Owner / Data Controller Data Custodian

ARTICLE 8
Training and Awareness

All College personnel are required to complete mandatory training on data classification, handling, and protection on an annual basis. This training ensures that staff understand their responsibilities regarding organizational data and follow the best practices in managing it. Additionally, role-specific training is required for individuals handling Restricted or Confidential data.

Training completion is monitored by each employee's immediate supervisor and overseen by the appropriate Service Director to ensure full compliance across all departments.

ARTICLE 9
Roles and Responsibilities

9.1 Board of Governors

The Board of Governors is responsible for approving the present Policy and ensuring that the College meets its legal and regulatory obligations concerning data governance.

9.2 Director General

The Director General is the ultimate authority over all organizational data and is accountable for the College's compliance with relevant legislation, ministerial directives, and internal policies. The Director

General ensures the appropriate allocation of resources to implement data protection measures and fosters a culture of accountability.

9.3 Director of Information Systems and Technology (IST)

The Director of IST is responsible for developing, implementing, and maintaining the technical and procedural framework required to protect data. This includes establishing security protocols, monitoring compliance, leading awareness initiatives, coordinating audits, and advising senior management on risks and mitigation strategies.

9.4 Senior Management

Senior management is responsible for operationalizing the present Policy within their departments by designating Data Owners and Stewards, ensuring appropriate data classification, and supporting secure handling practices. They are also expected to collaborate with IST and ensure that all staff under their authority receive proper training.

9.5 Users

All users are responsible for understanding and complying with the data classification and handling rules outlined in the present Policy. Users must protect the data they access, follow internal procedures, report any suspected breaches or misuse, and complete required training.

ARTICLE 10
Revisions

The present Policy shall be reviewed at least every five (5) years, or when deemed necessary by Ministry requirements or by the Board of Governors.