
<i>Policy No. & Title:</i>	C109: DATA CLASSIFICATION AND PROTECTION POLICY
<i>Effective:</i>	2026-09-24
<i>Next Review:</i>	2027-09-24 **ANNUAL REVIEW REQUIRED**
<i>Policy Sponsor:</i>	Vice-President, Corporate Services and Infrastructure
<i>Approvals:</i>	2026-09-24

1. PURPOSE

College information enables teaching, learning, research and operations and must be protected in a way that is proportionate to risk. This policy establishes a high-level consistent framework to classify information, assign accountability and apply safeguards that reduce unauthorized access, disclosure, alteration, loss or misuse. It sets required outcomes rather than prescribing a single technology or process, allowing controls to mature as risks, legal obligations and College capabilities evolve.

This policy is informed by and supports the College's alignment with the NIST Cybersecurity Framework 2.0 and applicable information security and privacy control practices reflected in ISO/IEC 27001 and ISO/IEC 27002. Supporting standards and procedures will define the controls and implementation requirements applicable to College information, systems and services.

This policy requires College information to be classified according to sensitivity and risk, protected throughout its lifecycle, accessed and shared only for authorized College purposes, and reported immediately when loss, inappropriate disclosure or unauthorized access is suspected.

2. SCOPE

This policy applies to employees. It also applies to contractors, volunteers, consultants and third parties who create, access, use, store, and transmit or dispose of college information on behalf of the College. Students are subject to this policy when they access or handle College information through employment, research, placements, clinical activities, governance or other authorized College activities. Ordinary coursework, assignments and other materials created by students are not subject to classification under this policy unless they contain College information, personal information or information governed by legal, ethical, research or contractual requirements. This policy covers College information in any physical or digital format and location, whether on premises, in the cloud or within college or third-party platforms and services.

3. DEFINITIONS

Data Loss Prevention (DLP): A set of policies, processes and technologies used to detect and prevent the unauthorized disclosure or loss of sensitive information.

Data Steward: The designated administrative or academic leader responsible for decisions about information within an assigned function or data domain, including classification, access, sharing, retention, disposal, data quality, and appropriate use. The role may be supported by operational delegates but remains accountable for decisions made under this policy. If no formal Data Steward is identified, the senior administrative or academic leader for the area that creates or primarily uses the data will assume the role or identify the appropriate leader.

Sensitive Data: College information classified as Confidential or Restricted under this policy. This includes information whose unauthorized access, use, disclosure, alteration, loss or destruction could harm an individual or the College, create legal, regulatory, ethical or contractual exposure, or materially disrupt operations. Information remains subject to applicable legal, regulatory, ethical and contractual requirements regardless of its classification.

COLLEGE POLICY MANUAL

Data Classification: The categorization of information according to its sensitivity, obligations and required level of protection as Public, Internal, Confidential or Restricted.

4. ROLES AND RESPONSIBILITIES

Employees and other users subject to this policy

- Comply with DLP requirements and data classification standards
- Use approved systems for storing and sharing sensitive data
- Report suspected data loss, inappropriate disclosure, or unauthorized access to Information Technology Services (ITS) and the Privacy Office immediately upon discovery.

Managers

- Ensure staff are trained and aware of DLP requirements
- Enforce compliance within their departments

Information Technology Services (ITS)

- Implement and maintain DLP technologies and supporting standards, monitor and respond to DLP alerts, secure endpoints and systems, and conduct applicable technology risk assessments and assurance activities.

Privacy Office

- Define data protection requirements aligned with the Freedom of Information and Protection of Privacy Act (FIPPA)
- Provide guidance on handling data according to the classification of the data
- Support incident response and breach assessment

Data Stewards

- Define and classify data within the given data domain
- Approve exceptions to the data classification standards and DLP requirements

5. DATA CLASSIFICATION AND HANDLING

All College information must be classified and handled as follows:

Classification	When to use and examples	Minimum handling requirements
Public	Approved for unrestricted public release. <i>Examples:</i> published web content, news releases, public reports, course calendars (excluding instructor and classroom details), course outlines, public event information and marketing material.	May be shared publicly after approval by the accountable Data Steward. Protect integrity and use approved College repositories.
Internal	Routine College information not intended for public release where disclosure would cause limited harm. <i>Examples:</i> internal procedures, routine operational communications, curriculum, draft agendas, internal directories, non-sensitive working documents and general training material.	Access is limited to the College community or authorized partners. Store and share through approved College systems. External sharing requires a valid business purpose and authorization from the accountable Data Steward.

COLLEGE POLICY MANUAL

Classification	When to use and examples	Minimum handling requirements
Confidential	Sensitive information where unauthorized disclosure could harm an individual or the College, create legal or contractual exposure, or materially disrupt operations. <i>Examples:</i> student and employee records, identifiable personal information, course assessment material, financial and procurement records, contracts, security assessments, non-public executive or Board material, donor information, identifiable research data and investigation files.	Access is limited by role and need-to-know. Use approved systems, strong authentication and encryption in transit and at rest where supported. Verify recipients before sharing. Do not use personal email, consumer file sharing, unapproved removable media or unapproved AI services. Securely dispose of paper and electronic copies.
Restricted	The most sensitive information, where compromise could cause severe harm, create significant regulatory exposure or threaten safety or critical operations. <i>Examples:</i> personal health information, government identifiers, payment card data, banking credentials, authentication secrets and private keys, highly sensitive legal or labour relations records, active incident details, critical security configurations, and research data subject to strict ethical, legal or contractual controls.	Access requires explicit authorization from the accountable Data Steward and must be limited to named individuals or tightly controlled roles. Use only specifically approved systems and encrypted channels. External sharing, use in AI, local storage, printing or removable media is prohibited unless formally approved with documented safeguards. Logging and monitoring must be enabled where technically available.

Data Stewards must review classification decisions at least annually and when material changes occur to the information, its sensitivity, source system, administrative use, legal or regulatory obligations, or the potential impact of unauthorized disclosure, alteration, loss or misuse. Classification reviews may be incorporated into broader assurance or audit activities and must be retained as evidence.

Classification identifies the sensitivity and required protection of information. It does not, by itself, grant access. Access to information at every classification level must be authorized, necessary for a legitimate College purpose and limited to those who require it to perform their responsibilities.

6. INFORMATION PROTECTION AND CONTROL ASSURANCE

The College will maintain a risk-based program of administrative, technical and physical safeguards. Supporting standards and procedures will define implementation details and may vary by information type, system, legal obligation and risk. Safeguards must be sufficient to prevent, detect, and respond to inappropriate access, use, disclosure, alteration, loss, or destruction, and must be reviewed as risks and capabilities change.

Required control outcomes

- Information is inventoried and classified at a level appropriate to institutional risk.
- Access is authorized, limited to need and reviewed periodically.
- Confidential and Restricted information is stored only in approved physical or digital locations, has an accountable Data Steward, and is accessible only to authorized individuals with a legitimate College need. It must be protected during storage, use, transmission and disposal.
- Systems and third parties handling sensitive information are assessed and approved according to risk.
- Control activity and material exceptions are recorded, monitored and retained as evidence.
- Suspected incidents are detected, reported, contained and reviewed.
- Users receive role-appropriate awareness and guidance.

Assurance and evidence: Accountable areas must be able to demonstrate compliance through evidence appropriate to the risk. Evidence may include assigned ownership, information inventories, classification decisions, access approvals and reviews, system or supplier assessments, training records, retention and disposal records, exception approvals, monitoring results and incident records. ITS and the Privacy Office may request evidence, assess control effectiveness and report material gaps to the accountable leader and Policy Sponsor.

Before a third party may access, process, store, or transmit Confidential or Restricted information, the proposed arrangement must undergo a security, privacy, and other risk review proportionate to the information and service. Applicable agreements must define required safeguards, permitted uses, access and subcontracting restrictions, retention and secure disposal requirements, audit or assurance rights, and obligations upon termination. Third parties must notify the College immediately upon discovering an actual or suspected breach, loss, unauthorized disclosure or security incident involving College information and must cooperate with containment, investigation, recovery and notification activities. Supporting procurement, security and privacy standards will define detailed requirements and approval processes.

7. ACCEPTABLE USE AND DATA SHARING

Users may share College information only when authorized, necessary for a legitimate College purpose and appropriate for the recipient. Confidential and Restricted information must be sent through approved College platforms, with access limited to the intended recipients. Recipient identity and permission must be verified before sharing. Information must not be stored or transmitted through personal accounts, consumer file-sharing, unapproved applications, unapproved artificial intelligence services, or unapproved devices.

Classification under this policy does not determine whether information is accessible or exempt from disclosure under the Freedom of Information and Protection of Privacy Act. Requests for access must be assessed through the College's established freedom of information process under the responsibility of the Privacy Officer. Information must not be disclosed solely because it is classified as Public or Internal.

Approved College platforms currently include Microsoft 365, Ellucian Colleague, Perceptive Content, Jadu, Workday, Shared Drive, and D2L when used for their intended institutional purposes. ITS may approve additional platforms and will maintain and communicate current guidance on approved applications.

Sensitive information must not be copied to or stored on USB drives, external hard drives or other removable storage unless a documented exception has been approved by ITS and the accountable Data Steward.

Sensitive information must not be entered into, uploaded to, processed by or used to train an artificial intelligence service unless the service has been institutionally approved for that classification and appropriate privacy, security, contractual, retention and access safeguards are in place. Approval of an artificial intelligence service for one purpose or classification does not authorize other uses.

If information contains elements from more than one classification, the highest classification applies to the complete record or data set. Information must be retained in accordance with the College records retention schedule, legal hold, contract or approved organizational need, and securely disposed of when the applicable retention requirement has been met and the information is no longer required for an authorized purpose.

8. MONITORING AND ENFORCEMENT

ITS, with input from the Privacy Office, Legal Counsel where required and accountable Data Stewards, will report annually to the Policy Sponsor on implementation, classification reviews, material risks, exceptions, incidents, control effectiveness and remediation. Material risks and significant non-compliance must be reported sooner. Non-compliance may result in proportionate access restrictions, corrective or disciplinary action up to and including termination of employment, contract remedies, legal action or regulatory reporting.

ITS may require technical safeguards, evidence of compliance, proportionate access or service restrictions, and remediation where information or systems face unacceptable risk. ITS may act without prior notice to contain a suspected incident, prevent material harm, meet a legal or regulatory obligation, or protect College operations. Significant restrictions and unresolved non-compliance must be reported to the Policy Sponsor and escalated through the appropriate College process.

9. INCIDENT REPORTING AND RESPONSE

Suspected data loss, inappropriate disclosure or unauthorized access must be reported to ITS and the Privacy Office immediately upon discovery. Users must not delay reporting while investigating, attempt to conceal an incident, or delete relevant evidence. The College will contain, assess, document and respond to the incident in accordance with its privacy breach and cybersecurity incident response processes, including notification obligations where applicable.

Exceptions: Exceptions must be approved by the accountable Data Steward and ITS before the activity occurs, with specialist input where required, and must document the organizational need, affected information and systems, risk, compensating safeguards, accountable Data Steward, approval and expiry date. Escalation to the Policy Sponsor is mandatory for Restricted information, high residual risk, actual or potential regulatory exposure, or exceptions extending beyond 12 months, including renewals. Exceptions must be time-limited, centrally recorded and reviewed at expiry. Emergency action to protect life, safety or College operations must be reported as soon as practicable.

The Policy Sponsor must ensure this policy is reviewed at least annually and following significant regulatory, security, privacy, technology or institutional change, with required amendments advanced through the applicable approval process.