AD30	Information Classification and Handling
Classification:	Administration
Responsible Authority:	Chief Digital Officer
Executive Sponsor:	Vice President, Human Resources
Approval Authority:	Algonquin College Executive Team
Date First Approved:	New
Date Last Reviewed:	2026-03-20
Date to Complete Mandatory Review:	2027-09-20

PURPOSE

This policy provides a framework for safeguarding the College's information assets by classifying them based on their value and the potential consequences of unauthorized disclosure.

SCOPE

This policy applies to all college community members who access, manage, or process information assets in all formats on behalf of the College.

This policy supports the College's commitment to transparency of operations and aligns with the principle of transparency by default as outlined by the Information and Privacy Commissioner of Ontario (IPC), while ensuring appropriate protection of information based on its classification.

DEFINITIONS

Word/Term	Definition
Asset	An Asset is anything, whether tangible or intangible, that has value to the College.
Classification	The process that allows the College to measure the value of information assets by assessing the potential risks and consequences of their unauthorized disclosure.
College Community	The College Community refers to Algonquin College students, employees, volunteers, and contractors.
Information	Information is processed, structured, or interpreted data that has meaning and value within a specific context.
Information Custodian	A person or role responsible for implementing and maintaining the technical and procedural safeguards to protect information assets as directed by the Information Owner.

Information Owner	A person or role responsible for defining the classification, access, and protection requirements of information assets within their department to align with business objectives and regulatory obligations. They set the policies that dictate how information should be managed and secured.
Processing	Processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, use, and disclosure. Use includes recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, matching or combining, restricting, erasing, and disposing.

POLICY

1. Roles and Responsibilities

Information Owners are accountable for classifying and protecting information assets based on their respective classification levels as defined in this policy.

Information Custodians shall implement the appropriate controls, access restrictions, and safeguards to ensure compliance with the handling requirements based on the information's classification level.

Information Technology Services, in alignment with the Enterprise Risk Management Framework, shall identify, assess, audit, and mitigate risks associated with information classification and handling to prevent the unauthorized disclosure or modification of classified information.

The **College Community** shall adhere to all College Policies, and information classification and handling requirements, reporting any potential incidents, non-compliance or violations of this policy to the Information Technology Services Department.
All **College employees** must complete the mandatory Information Classification and Handling training provided.

If an Information Owner or Custodian is unsure how information should be classified or handled, they should discuss it with their supervisor and contact Information Technology Services for guidance if necessary.

Failure to comply with this policy may result in corrective or disciplinary actions in accordance with the College policies, including the Employee Code of Conduct policy (HR18).

2. Information Classification

The **College** shall classify any information it processes based on the potential impacts from improper or unauthorized disclosure on the College's or College Community's safety, finances, operations, regulatory compliance and reputation.

All College information shall be classified as **Internal** by default, unless and until the Information Owner has reviewed the information and assigned an appropriate classification level.

These four classification levels will ensure risk-based safeguards are in place to mitigate the impacts of unauthorized disclosures on the College:

Classification Levels	Risk of unauthorized disclosure	Definition	Potential Example
Public	Level 0 – Low	Information that is intended for public access, poses no risk to the College if disclosed, and is meant for widespread dissemination.	• Faculty and staff directory information • Course catalogues • Published research data • Advertised Jobs and Tenders • Corporate Policies
Internal	Level 1 – Medium	Information that is restricted to internal College use. Unauthorized disclosure would have moderate impacts on the College's or College Community's safety, finances, operations, regulatory compliance and reputation.	• Class Lists • ITS, Facilities and security system design and configuration information • Contractual agreements that include a confidentiality clause, are subject to a non-disclosure agreement, or include information which is not otherwise publicly available • Information related to a regulator's request that could be damaging to the College and is not otherwise subject to Freedom of Information
Confidential	Level 2 - High	Information that is critical to the College's operations. Unauthorized disclosure would have high impacts on the College's or College Community's safety, finances, operations, regulatory compliance and reputation.	• Exam materials and results • Personal information identifying or reasonably linking to an individual and, if disclosed without authorization, could result in harm to the individual or the organization. Example includes any combination of identifiers such as student/employee ID and/or name with sensitive demographic information or student record data • Organizational financial data that is not otherwise publicly available • Research data

			• Unpublished intellectual property • Payment and Credit Information • Contractual agreements deemed confidential under FIPPA
Restricted	Level 3 - Critical	Information that is highly sensitive and critical to the College. Unauthorized disclosure would have critical impacts on the College's or College Community's safety, finances, operations, regulatory compliance and reputation.	• Personal health information • Restricted Personal information such as government issued identification (Social Insurance Number (SIN), Passport...) • Information related to and identifying children and young persons • Research Data (containing personal and/or personal health information) • Solicitor-client privileged documents and communication • Litigation privilege documents and communications

3. Information Handling

The **College** shall implement appropriate handling measures to information based on its classification level, ensuring that information is protected according to its classification and potential impact if disclosed. This policy shall not limit the College's transparency obligations as defined under applicable legislation and contractual agreements.

The **College Community** must make themselves aware of, and adhere to, the handling practices described below for all College information assets, regardless of their classification to ensure their security and privacy:

- **Access**: Information must be accessed and handled only by those who require it to fulfill their role or responsibilities, based on the principles of least privilege and need-to-know.
- **Storage**: Information must be stored securely, with appropriate access restrictions in place to prevent any unauthorized access.
- **Transmission**: Information must be transmitted securely, using methods that ensure its confidentiality and integrity.
- **Retention**: Information must be retained in accordance with College-established retention policies and securely disposed of when it is no longer required for business or

regulatory purposes. Refer to existing retention policies (such as AA49 - Electronic Student Record Retention policy) where available.

- **Disposal:** Disposal methods must ensure that information is irretrievable after destruction as defined in the College's retention policies.
- **Auditing** : Information must be audited through comprehensive logs that record all user interactions, including the nature of access, timestamps, and user identification, with retention periods matching the information itself.

It is recommended that the College Community prioritize digital record keeping whenever reasonably possible to support secure, accurate, and cost-effective management of College information assets. Digital record keeping is highly recommended for all Internal, Confidential, and Restricted information.

Information and Information Handling associated with applied research and applied research projects must also comply with Ministry of Colleges, Universities, Research Excellence and Security (MCURES) regulations and any other governing legislations. In situations where applied research Information Handling is unclear, the Director, Applied Research will dictate.

The information handling practices outlined in this policy shall be reviewed periodically, and updated as necessary, to reflect technological changes, emerging threats, and newly identified risks.

Refer to the available Information Classification and Handling training and guide made available for further guidance.

3.1. Classification Based Information Handling Requirements

Classification Levels	**Requirements**			
	Access	**Storage**	**Transmission**	**Disposal**
Public	• No special access controls required.	• Information can be stored on general-purpose systems with basic security measures.	• Transmission can occur over standard networks without encryption. • For public-facing content, transmission leverage encryption.	• Simple deletion or recycling methods are acceptable.
Internal	• Limited to authorized users within the College.	• Information should be stored on College-approved	• Transmission should occur over secure networks.	• Information should be permanently deleted or overwritten

		systems with access controls. • Encryption recommended when stored on portable devices (media / disk)	• Encryption (College Virtual privacy Network - VPN) should be applied when transmitting over untrusted networks.	when no longer needed. • Physical records should be securely disposed of and considered for shredding using a College approved method or third-party service.
Confidential	• Restricted to authorized indi viduals with specific roles or approval.	• Information must be stored with strong access controls and encryption where feasible.	• Transmission should occur over secure networks with encryption applied. • Data shared externally must be protected via agreements and encryption.	• Information must be securely and permanently deleted or overwritten. • Physical records should be shredded using an approved method or third-party service.
Restricted	• Strictly limited to authorized individuals with specific roles and approval.	• Information must be stored with strict access controls and encryption. • Storage systems must have enhanced monitoring and audit logging.	• Transmission must be encrypted and use secure networks. • Data shared internally or externally requires explicit approval and must be protected via agreements and encryption.	• Information must be destroyed through approved methods or a third-party service that ensures irretrievability (e.g., degaussing, physical destruction).

Note: Detailed definitions of security controls, approved systems, encryption methods, and network classifications are provided in the Information Security Control Standard . Contact ***Information Technology Services*** *for guidance on implementing these requirements.*

3.2. Exceptions to Information Handling Requirements

In certain cases, exceptions from this policy may be necessary. Requests for exceptions must be submitted by the College Community to the Information Technology Services Department. All exception requests should be submitted through the appropriate form, and must include:

- A rationale for the exception.
- An assessment of the associated risks.
- Compensating controls, if applicable.
- The duration of the exception.

Information Technology Services will review each exception submitted by the College Community on a case-by-case basis, and approval will be granted by the Information Owner or delegate only if the risks are mitigated appropriately.

SUPPORTING DOCUMENTATION

None

RELATED POLICIES

AA35: Confidentiality of Student Records
AD02: Freedom of Information
HR18: Employee Code of Conduct
IT01: Information Security

RELATED MATERIALS

FIPPA, Part II, Exemption
https://www.ontario.ca/laws/statute/90f31#BK23

Information classification and handling employee training

Information classification and handling guide

Information Security Control Standard