Policy Number:	**CS-1508-2020**
Policy Title:	**Information Governance and Security Policy**
Policy Owner:	**Chief Information & Technology Officer**
Effective Date:	**May 1, 2021**
Last Revised:	**June 29, 2026**

1. Purpose

This policy provides Mohawk College with direction on handling electronic and physical information with central and consistent guidance on creating, collecting, classifying, labelling, securing, storing, using, copying, transferring, and disposing of information. This policy also defines roles and responsibilities as it relates to the lifecycle and integrity of information.

2. Application and Scope

This policy applies to all employees, contractors, consultants, researchers, volunteers, or other workers including College community members that use any component of Mohawk College's information regardless of their role, location, device, or facility.

3. Definitions

"**Authorization**" is the act of approving access to information.

"Information" refers to all components of data within the custody and control of Mohawk College.

"Information Classification" is the activity of reviewing and applying a classification from this policy based on the sensitivity of the data itself to aid the College in proper data handling procedures.

"Electronic Information" refers to any component of information that is accessible on a computer system, application, cloud application, storage, or removable media.

"**Electronic Media**" refers to storage devices for computer systems which includes disk and solid state drives, USB drives, cd's, DVD's, and tapes.

"Personally Identifiable Information" is defined by the *Freedom of Information and Protection of Privacy Act* (FIPPA), as:

a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

c) any identifying number, symbol or other particular assigned to the individual,
d) the address, telephone number, fingerprints or blood type of the individual,
e) the personal opinions or views of the individual except where they relate to another individual,
f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
g) the views or opinions of another individual about the individual, and
h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

"**Provisioning Access**" means to modify controls to allow an individual to have access only after it has been authorized by a Data Trustee or Steward.

"Removable Media" refers to any device such as USB drives, disks, or tapes, among others that are capable of storing electronic information.

"Physical Information" refers to any paper or printed documents, drawings, blue prints, receipts, student or employee cards, and photographs that contain information.

"Safeguards" are physical, technical, or administrative security controls implemented to protect against unauthorized access to systems and information. Examples include, but are not limited to, locks with keys or combinations, secure rooms, video surveillance, card access, single factor or multifactor authentication, biometrics, user access control, network access controls, and contractual agreements, policies, procedures.

"**System Administrator**" is a user who manages the upkeep, operation, and configuration of a computer system or electronic communications system component. These users can be identified by having administrative privileges of a system or who has built or will build a system.

"Data Domain" and **"Functional Area"** both refer to a high-level category of information. Examples include Human Resources, Finance, Admissions, and Enrollment.

"Data Trustee" is a Senior Leadership Team (SLT) member who is accountable for what happens *with* and *to* college data within the data domains they are assigned ownership.

"Data Steward" is an individual or individuals who work closely with the data. This role is tasked with, among other things, managing the curation or collection of these data points, addressing data quality issues, and managing content and meaning of data elements within their data domain. For example, an Admissions data steward might be responsible for defining what is meant by "Application Status," as well as the valid reference data and appropriate usages for that concept.

4. PRINCIPLES:

Mohawk College collects, creates and maintains information to operate the College and is required to handle that information in a responsible manner through controls and data governance practices.

5. Accountability and Compliance

5.1 Accountability Framework
This policy has been approved by the Senior Leadership Team.

5.2 Compliance
This policy is aligned to the National Institute of Standards and Technologies Cyber Security Framework, ISO 27001, Freedom of Information and Protection of Privacy Act (FIPPA), Payment Card Industries Data Security Standards (PCI DSS), Data Governance best practices, and is enforced by the Chief Information & Technology Officer.

6. Roles and Responsibilities

6.1 Chief Information & Technology Officer
The Chief Information & Technology Officer is accountable for the security of all IT resources.

6.2 Data Trustees
SLT members act as Data Trustees for data within their Functional Area or Domain. Not every SLT member will have an assigned Data Domain. Data Trustees must work collaboratively across their departments to ensure that information is identified, classified, maintained, safeguarded, and disposed in compliance with this Policy working with Data Stewards and Custodians.

A Data Trustee delegates one or more individuals to act as Data Stewards for their data domain.

6.3 Data Stewards
Data Stewards are responsible for authorizing access to sensitive information and systems, maintaining functional data definitions, data quality, classification, security, and legislative compliance for data assets within their data domain(s), and participate in Data Governance committees and discussions.

The Data Steward is responsible for ensuring individuals that have access to sensitive information are aware of their responsibilities to protect that information described within this policy and ensure that sensitive information is not stored or collected without a formal plan to enforce the rules within this policy.

6.4 Data Custodians
An employee of the College with any level of operational authority, responsibility, expertise, and knowledge about a data source, application, or storage in their functional area.

Data Custodians are responsible for managing the technical environment and ensure the safe collection, custody, transport, storage, and destruction of the data. Custodians manage security controls and facilitate access after the Steward has authorized the request. Data custodians help manage technical data definitions – documenting where data resides within a system for a given functional term.

6.4.1 Information Technology Services
Information Technology staff act as Data Custodians and are responsible for supporting Data Trustees, Stewards, and departmental Data Custodians to deploy

the appropriate safeguards as defined in this Policy and the Information Technology Infrastructure Security Policy.

6.4.1.1 System Administrators

System administrators are responsible for deploying the appropriate technical safeguards in collaboration with Data Trustees, Stewards, departmental Data Custodians, and IT Security.

6.4.2.1 IT Security

IT Security is responsible for assisting Data Trustees, Stewards, and Custodians in identifying and classifying information and assisting system administrators with deploying technical safeguards along with participating in Data Governance activities.

IT Security further provides consultation services related to information security and is responsible for conducting information security audits.

6.5 Data Users

Data Users are individuals who have direct interaction with information as part of their assigned duties within the College and must ensure they use information in a manner consistent with its intended purpose and in compliance with this Policy and Governing Law.

6.6 Information Management Services

Information Management Services is responsible for the continuous oversight of policies, standards, and controls related to information governance along with monitoring compliance to this policy.

Information Management Services provides consultation and guidance with College stakeholders to develop or reform practices based on this policy, ensure information descriptions and flows are appropriately documented and ensure overall information integrity, privacy, and security are maintained throughout the information lifecycle.

7. RULES

7.1 Data Trustee Assignment

Data Trustees are assigned to the Data Domain(s) or Functional Area(s) for which they have operational oversight. This means not all SLT members will have an assigned data domain. This SLT member assumes the role of Data Trustee, shall delegate a Data Steward, and assumes responsibility for enabling the controls within this policy.

7.2 Collection and Use of Personally Identifiable Information

Personally Identifiable Information (PII) must only be used for the purpose(s) for which it was collected unless specifically authorized by the data subject. The PII must only be kept as long as required to serve its purpose, or, in accordance with legislative requirements, and then destroyed in compliance with this policy.

Where departments collect or retain information that includes PII, Data Trustees must explicitly identify the purpose for which personally identifiable information is being collected before and at the time of collection in a way in which individuals can understand and consent to. The collection of PII must be limited to that which is necessary to fulfill the intended business purpose and where the College has the legal authority to collect the information. Data Trustees must contact the Office of the General Counsel and Corporate

Secretary for creation of privacy disclaimers to address consent and any further guidance as required.

7.3 Classification of Information

Information must be classified in terms of sensitivity to the organization. Where multiple subsets of information are stored together, that information is classified at the highest level in the subset. Data Trustees, Stewards, Custodians, and Users will classify Information as categorized in Appendix A as:

Guidance	Classification	
Sensitive		RESTRICTED
		RESTRICTED HEALTH
		CONFIDENTIAL
		INTERNAL USE ONLY
Non-Sensitive		PUBLIC

7.4 Labeling of Restricted and Confidential Information

To support consistent information handling practices, information classified as Restricted, Restricted Health, and Confidential must be labelled with their information classification. Information classified as Internal Use Only or Public may be labelled at the discretion of the author.

7.4.1 Labeling of Electronic Information

Electronic files must be labelled using watermarking, headers, or adding additional text to the document.

7.4.2 Labeling of Physical Information and Removable Media

Printed documents and faxes must be labelled with their classification label. Where appropriate, departments may use the colour scheme to aid in labelling. Physical media such as USB drives or disks which are encrypted using strong encryption in compliance with the Requirements for Encryption Policy do not require labelling.

7.5 Safeguarding of Sensitive Information

Data Trustees are required to ensure that appropriate safeguards are put in place which include technical, physical, and administrative safeguards as necessary and the below points are not exhaustive.

7.5.1 Safeguarding of Electronic Information

Electronic sensitive information must be stored on authorized College systems and not stored locally on desktops and laptops (ex: Use Onedrive, H: Drive, or Department shares, not My Documents). System Administrators must configure systems that safeguard sensitive information in compliance with the Information Technology Infrastructure Security Policy.

7.5.2 Safeguarding of Physical Information and Removable Media

Physical information and removable media containing sensitive information must be stored in a secure location when unattended. Acceptable secure storage includes

locked safes, rooms, file cabinets, inside of desks, or other secured containers under lock and key. Stored information must only be kept when there is legitimate business purposes to reduce the threat of theft and risk of inappropriate disclosure and potential breach of personally identifiable information.

Removable media storing sensitive information should be avoided where possible. Strong encryption must be used to protect information stored on any portable media in compliance with the Requirements for Encryption Policy.

7.6 Providing Access to Sensitive Information

Access to sensitive information must be authorized on a need to know basis, and may be based on job role. Users must request access to information and authorization must be performed by a Data Trustee or Data Steward. Electronic access is provisioned by custodians once authorized.

7.7 Copying or Moving Confidential and Restricted Information

Never copy, move, duplicate, or relocate sensitive information without approval from the originating Data Trustee. If approved the Data Trustee overseeing the relocation is responsible for complying with all provisions of this policy.

7.8 Creating and Maintaining High Quality Information

Information must be collected, created, modified, and maintained with assurance that the Information quality and integrity is accurate, complete and consistent with business requirements such that it can be used for its intended purpose and reporting requirements. Information identified to be of low quality must be corrected at its source and replicated to down stream systems where appropriate. Departments must maintain business documentation such as training materials, standards, controls, information flows, and retention schedules for information under their stewardship.

7.9 Transfer of Sensitive Information to Third Parties

Transferring sensitive information outside of the College must be in compliance with Mohawk College's Privacy and Legal Statements, and, where that information includes Personally Identifiable Information, that transfer must be consistent with legislative requirements. Data Trustees should consult with the General Counsel and Corporate Secretary's Office, or the IT Security Department for guidance as appropriate.

7.9.1 Electronic Transfer of Personally Identifiable Information

Strong encryption must be applied to electronic transfers in compliance with the Requirements for Encryption policy.

Electronic Transfer of non-encrypted personally identifiable information outside of the College via end-user technologies (i.e. e-mail, instant messaging, or SMS) is strictly forbidden when the transfer is not direct to the information subject.

7.9.2 Physical Transfer of Personally Identifiable Information and Media

Transportation of Personally Identifiable Information on documents and removable media to other organizations or third parties should be avoided where possible. If required, a chain of custody log must be created, stored, maintained, and updated using the example log sheet in Appendix B.

7.10 Disposal of Sensitive Information

7.10.1 Disposal of Physical Sensitive information

Paper documents containing sensitive information must be disposed of using a crosscut paper shredder, or through the Shipping and Receiving Department using secured and locked disposal bins. Sensitive information on paper must never be disposed of in recycling bins. When working remotely physical sensitive information must be kept secure until an acceptable method of destruction is available.

7.10.2 Disposal of Electronic Sensitive Information

Electronic media containing sensitive information must be delivered to the IT Service Desk for secure disposal or reuse in compliance with the IT Electronic Media Disposal and Re-use Procedure.

7.10.3 Documenting Disposal of Personally Identifiable Information

When a department disposes of Personally Identifiable Information (i.e. stored records in boxes or decommissioned databases or datasets etc.), a data disposal log must be filled out (Appendix C) and retained by the destroying department. This requirement does not apply to transient customer service transactions such as an individual registration form or letter.

7.10.4 Legal Hold

Where information is subject to a legal hold it can not be deleted until authorized by General Counsel

7.11 Accidental Loss or Inappropriate Disclosure of Sensitive Information

Loss or disclosure of sensitive information must immediately be reported to Information Technology following instructions in the Acceptable Employee Use of IT Resources Policy and handled following incident response procedures.

7.12 Awareness and Right to Audit

Upon request of the CITO, Data Trustees must perform access audits to ensure that only the correct and authorized users have access to sensitive information under their control. The CITO, Internal Audit, Legal, Privacy, Cyber Security, and Information Management Services may conduct information governance, security, or privacy audits at anytime to validate controls against this policy and any laws, regulations, policies, standards, and procedures.

8. Policy Revision Date

8.1 Revision Date

June 2031

8.2 Responsibility

The Chief Information & Technology Officer will review this policy every five years or earlier where required.

9. Attachments

Appendix A – Data Classification Table
Appendix B – Physical Transfer Chain of Custody Log Sheet
Appendix C – Disposal of Personally Identifiable Information Log

10. Specific Links

SS-3106-1978 Access to Student Records
CS-1502-2002 Acceptable Employee Use of IT Resources
GC-4101-2013 Copyright

GC-4100-2013 Intellectual Property and Commercialization Principles Policy
Privacy and Legal Statements
Academic Collective Agreement
Support Staff Collective Agreement
Terms and Conditions of Employment for Administrative Staff
Employee Code of Conduct
Copyright Act
Information Technology Security Standards (Available Upon Request)
IT Electronic Media Disposal and Re-use Procedure (Available Upon Request)

Appendix A
Data Classification Table

The following table provides guidance on selecting an Information Classification and what type of Access and Storage Requirements that Classification level is subject to:

Sensitive		**This Information may contain Personally Identifiable Information (PII)** **RESTRICTED:** Restricted information is information that if disclosed to unauthorized parties could have serious legal repercussions or negative reputational consequences. Restricted information requires the highest level of protection and is typically only accessed and used by a small number of individuals on a need to know basis. This classification includes any federal or provincially issued components of Personally Identifiable Information (PII).

Access: is strictly controlled to only limited authorized employees and is revoked immediately when no longer required by Job Function or Need to Know.
Storage: Physical copies must be stored in restricted areas of the College and monitored. Electronic information must be stored on College servers or Cloud solutions protected by the appropriate contractual agreements. Storage on computers and laptops should be avoided.
Examples: SIN, Drivers License, Health Card Number, Financial Account Numbers, Credit Card Numbers, Passwords, Private Encryption Keys, Board Materials, Financial Information, Human Resources Information, Applied Research Projects, Intellectual Property of others.

Sensitive

This Information may contain Personally Identifiable Information (PII)

RESTRICTED HEALTH: Any Personally Identifiable Information (PII) about an individual that relates to the physical or mental health of that individual, including health history of the individual's family. This also includes information about the care provider, plans for long term care, payments or eligibility for health care, and the individuals PII. See PHIPA Legislation for more details.

Access: is strictly controlled to only limited authorized employees and is revoked immediately when no longer required by Job Function or Need to Know.
Storage: Physical copies must be stored in restricted areas of the College and monitored. Electronic information must be stored on College servers or Cloud solutions protected by the appropriate contractual agreements. Storage on computers and laptops should be avoided. Additional legislation exists protecting cross border transactions of Restricted Health Information – Consult with Legal, Privacy, and IT Security related to any offsite storage including Cloud technologies. Storage on computers and laptops should be avoided.
Examples: Patient Name's, Health Card Information, Date of Birth, Address, Contact Information, Billing Information, Prescription Costs, Counselling Information, Physician Notes, Test Results, Medical Images

Sensitive

This Information may contain Personally Identifiable Information (PII)

CONFIDENTIAL: Confidential information includes important information about Mohawk College employees and students, and highly sensitive internal information. This category includes all Personal Identifiable Information (PII) that is not classified as restricted.

Access: is controlled to small groups of staff who require access to the information to carry out their job roles. Access must be revoked when no longer required by job function.
Storage: Physical copies must be stored in restricted areas of the College and monitored. Electronic information must be stored on College servers or Cloud solutions protected by the appropriate contractual agreements. Storage on computers and laptops should be avoided. Storage on Computers and Laptops should be avoided.
Examples: First Name, Last Name, Address Information, phone number, e-mail address, Date of Birth, Age, Mohawk ID, photograph, biometric information, Financial Information about Mohawk College, Infrastructure Details about Mohawk College, IP Addresses, etc.

Sensitive		**INTERNAL USE ONLY:** Data or documentation that is used by Mohawk College for day-to-day processes and functions and is not intended for public distribution. Data Users should be cautious with whom this information is shared with. **Access**: is provided to employees and other authorized individuals for business related purposes. **Storage**: Physical and Electronic copies may be stored as securely as determined by the owner based on the context of the document. **Examples:** Internal procedures, guidelines, meeting agendas, documentation.
Non-Sensitive		**PUBLIC:** Information that if shared, has no known or associated risks. Public information is available outside of our organization and is intended for public use. Data Users can share this information with everyone. **Access**: is for everyone. **Storage**: can be anywhere. **Examples:** Marketing Information, Campus Maps, Corporate Policies and Procedures, Program Information, Mohawk College Website, Advertisements, etc.

Appendix B
Example Physical Transfer
Chain of Custody Log Sheet

To be used in compliance with 7.9.2 of the Information Security and Classification Policy

Date	Name of Receiving Entity	Address of Receiving Entity	Contact Information of Receiver	Name and Job title of Sender	Reason for Transfer	Method of Transfer

Appendix C
Example Disposal of Personally Identifiable Information Log

To be used in compliance with 7.10.3 of the Information Security and Classification Policy. The log shall include the following information, at a minimum, in alignment with the Data Disposition Log:

Field	**Description**
Data Source Name / ID	Unique identifier for legacy system
Data Trustee	Accountable business leader
Data Steward	Individual conducting assessment
Assessment Date	Date of evaluation
Recommended Disposition	Migrate / Warehouse – Reporting / Warehouse – Cold Storage / Archive / Destroy
Justification	Business, analytical, and compliance rationale
Legal Review	Name and date of legal/compliance reviewer
Data Governance Committee Approval	Record of approval (meeting minutes or digital sign-off)
Execution Completed By	Team or individual performing action
Evidence	Migration logs, archive confirmation, Ticket or RFC #, or destruction certificate