Policy Title:	Electronic Information Security Policy
Policy ID:	6-604
Manual Classification:	Section 6 – Information Technology
Approved by:	Board of Governors
Revision Date(s):	2022-06-22
Effective Date:	2022-07-01
Next Policy Review Date:	2025-06-01
Contacts for Policy Interpretation:	CTO Directors, Information Technology

1.0 - Policy Overview

This policy (the "**Policy**") provides Fleming College with direction on the confidentiality and integrity of the College's electronic information assets and records. Fleming College collects, creates, and maintains information to operate the College, and is required to manage that information in a responsible manner through data governance practices and controls.

2.0 - Purpose

This policy outlines the responsibilities of members of the College Community with respect to the classification of electronic information and appropriate safeguard to protect the confidentiality, integrity, and availability of the College information.

3.0 - Definitions and Acronyms

All Users	The set of all individuals who use Fleming College IT systems or resources, usually via a designated user account.
Application or System Administrator	Any user who manages the upkeep, operation, and configuration of an electronic system or application. These users can be identified by having administrative privileges over the system or application.
College Community	All people who study, teach, conduct research at or works at, or under, the auspices of the College and includes without limitation: employees, contractors; appointees (including volunteer board members); students; visitors; and any other person while they are acting on behalf of, or at the request of the College.
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 data creation, collection, classification, labeling, safeguarding, provisioning access, copying, moving, and disposing of

	data, at an operational level in their functional area in compliance with this policy.
Data Stewards	Any administrative employee of the College that ensures individuals that have access to sensitive information are aware of their responsibilities to protect that information as described in this policy.
Data Trustee	A senior administrative employee that has responsibility for a functional area of the College and any records related to that function. The Data Trustee is accountable for ensuring that its records are maintained according to this policy. (See related definition of Office of Primary Interest.)
ISMS	An Information Security Management System is a systemic approach to managing sensitive organization information so that it remains secure. It is comprised of people, processes, and technologies that manage the overall security of the organization's systems and data.
IT Standards	IT Standards are specific and granular requirements that give direction to support broader-level IT policies.
Office of Primary Interest (OPI)	In alignment with the Canadian Library and Archives, the OPI is the office or department that has the main responsibility for a subject area and any related records. The OPI, as the primary Data Trustee, is accountable for ensuring that its records are maintained according to College Policy, Operating Procedures, and Standards. For example, the department responsible for the recording of minutes by a committee would be considered the OPI and must ensure that those records are properly classified and protected.

4.0 - Scope

This policy applies to all members of the College Community that use any Fleming College information regardless of their role, location, device, or facility.

5.0 - General Principles

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

All College records produced by employees in the normal course of operations belong to the College.

Information collected is to be used only for defined or approved purposes.

5.1 - Roles and Responsibilities

Protection of the College's electronic information, information systems and infrastructure are responsibilities shared by all members of the College Community. All Users are expected to follow this policy, related operating procedures, and ITS Standards.

Chief Technology Officer (CTO) and ITS Directors

The Chief Technology Officer is accountable for the security of all information technology (IT) resources.

The CTO is accountable for oversight of the information security management system (ISMS) to ensure the ongoing confidentiality, integrity, and availability of the College's electronic information systems. The ISMS will align with the College's Enterprise Risk Management Policy and ISO/IEC 27001:2013 as a framework standard.

The ITS Directors are responsible for implementing, maintaining, and continually improving the security of Fleming IT infrastructure, applications, the information security management system (ISMS), and related controls. Further specific responsibilities are identified by related operating procedures.

Senior Management Team (SMT) as Data Trustees

SMT members, as leaders of their respective departments and offices of primary interest (OPI), act as Data Trustees, where their department(s) collect, create, modify, copy, move, transfer, share, or dispose of college information. Data Trustees must work collaboratively across their departments to ensure that information is identified, classified, maintained, safeguarded, and disposed of in compliance with this policy, working with Data Stewards and Data Custodians.

Managers as Data Stewards

Managers act as Data Stewards and must ensure individuals under their oversight who 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.

Data Stewards are responsible for authorizing access to sensitive information and systems in compliance with this policy and the related operating procedure #6-604B, Access Control.

Information Technology Services (ITS)

ITS staff act as Data Custodians and are responsible for supporting Data Trustees, Data Stewards, and departmental Data Custodians, to implement and maintain, appropriate safeguards as defined by this policy.

System and Application Administrators

System and Application Administrators are responsible for deploying the appropriate technical safeguards in collaboration with Data Trustees, Stewards, Custodians, and IT security.

5.2 – Data Governance Committee

The CTO will appoint a Data Governance Committee with responsibility for:

a) Continuous oversight of policies, procedures, standards, and controls related to information governance along with monitoring compliance to this policy.
b) Providing consultation and guidance to college stakeholders to develop and inform data handling practices based on this policy.
c) Review and agree on appropriate uses for College data assets

d) Review and confirm the Information Classification Levels assigned by Data Trustees and/or Data Stewards.
e) Review and approval of data-sharing agreements.
f) Maintaining an Inventory of Records, for all sensitive electronic records and related data systems. The inventory will include at a minimum: record type, system name, classification level, storage location, retention and disposition requirements, OPI, Data Trustee(s), Data Steward(s), and Data Custodian(s).

5.3 – Emergency Authority
In the event of an emergency that threatens information security of the College, the President (or designate), or CTO (or designate), shall have full authority to enact emergency response measures. If deemed necessary, to mitigate damage to, or inappropriate disclosure of, College information assets, appropriate actions may include but are not limited to, a full shut down of all information and communication systems.

5.4 – Personal Information
College Policy, Operating Procedures, Standards, and processes, for the collection and management of personal information, are defined based on and are subordinate to, Personal Information Protection and Electronic Documents Act (PIPEDA), the Freedom of Information and Protection of Privacy Act ("FIPPA") and College Policy 1-111 Access to Information and Protection of Privacy.

5.5 – Health Information
College Policy, Operating Procedures, Standards, and processes, for the collection and management of health information, are defined based on and are subordinate to, the Personal Health Information Protection Act, 2004 ("PHIPA") and College Policy 1-112 Information Practices Related to Personal Health Information.

5.6 – Classification and Safeguarding of Electronic Information
College Information must be classified in terms of legal requirements and sensitivity to the organization. A risk-based approach to information classification aligned to the College's Enterprise Risk Management Policy will provide risk guidance in determining appropriate safeguards and controls for various classification levels.

The CTO is responsible for the implementation of the College's information security operating procedures for information classification and access controls. These will include but not be limited to:

- Information Classification Levels
- Security Protections for Information Classification Levels
- Labeling of Information
- Access Control (Governance, Implementation, Review)
- Safeguarding of Sensitive Information
- Providing Access to Sensitive Information
- Copying or Moving Sensitive Information
- Creating and Maintaining High Quality Information
- Transfer of Sensitive Information to Third Parties
- Record Retention and Disposition
- Disposal of Sensitive Information
- Accidental Loss or Inappropriate Disclosure of Sensitive Information
- Information Security Incident Management

5.7 – Awareness and Right to Audit

Upon request of the CTO or the Data Governance Committee, Data Trustees must perform access audits to ensure that only the correct and authorized users have access to sensitive information under their control. The CTO, Internal Audit, Legal, Privacy, and IT Security staff among others, acting on behalf of the College may conduct information governance, security, or privacy audits at any time to validate controls against this policy and any laws, regulations, policies, standards, and procedures.

6.0 - Related Documents

- PIPEDA – *Personal Information Protection and Electronic Documents Act* (2000)
- FIPPA - *Freedom of Information and Protection of Privacy Act* R.S.O. 1990 c. F. 31
- PHIPA – *Personal Health Information Protection Act* (2004)
- College Policy #1-108*,* Enterprise Risk Management
- College Policy #1-111, Access to Information and Protection of Privacy
- College Policy #1-112*,* Information Practices Related to Personal Health Information
- College Policy #6-600, IT Policy Framework
- College Policy #6-601, IT Appropriate Use Policy
- College Policy #9-904, Intellectual Property and Copyright
- College Operating Procedure #6-604A, Information Security Classification Procedure
- College Operating Procedure #6-604B, Access Control Procedure
- College Operating Procedure #6-604C, Incident Security Incident Management
- International Organization for Standardization, Information security management systems – Requirements - ISO 27001

History of Amendments/Reviews

This policy, and its subordinate operating procedures, supersedes previous College Policy #6-603*,* College Data Record Retention and Disposition