

Policy Title:	Record Retention
Policy ID:	1-104
Manual Classification:	College Policies
Approved by Board of Governors (BoG):	May 28, 2025
Effective Date:	June 1, 2025
Next Policy Review Date:	May 28, 2028
Contacts for Policy Interpretation:	Vice President, Information Technology & Digital Strategy

1.0 - Policy Overview

This policy provides guidance for the retention, destruction and archiving of records within the College's custody and control, supported by associated retention schedules and OP 1-104.

2.0 - Purpose

The purpose of this policy is to ensure compliance with legal, regulatory, and College policies; promote efficient record-keeping practices; and ensure the confidentiality, consistency, and integrity within the management of College records.

3.0 - Definitions and Acronyms

Access: The right or opportunity to, or means of, reading, copying, querying, finding, or retrieving Records.

Active Records: Records created or received in the course of College operations that are regularly used to conduct business activities. These Records are maintained in the Office of Primary Interest (OPI) for their entire life and remain under the custody, responsibility and control until change in destruction occurs.

Archived Records: Records that serve as the evidence of the College's historical activities and act as its institutional memory, which are not to be destroyed.

College Community: Any person who studies, teaches, conducts research at or works at or under the auspices of the College and includes without limitation: employees or 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.

Device: Any Internet-capable computer hardware device that could connect to the College network and includes desktop computers, laptops, smartphones, tablets, thin clients, printers, faxes, scanners, or other specialized hardware.

Destruction: The secure destruction of a record per its RRS.

FIPPA: The Freedom of Information and Protection of Privacy Act (R.S.O. 1990, c. F.31) is an Act of the Legislative Assembly of Ontario. The Act legislates access to information held by public institutions in Ontario subject to specific requirements to safeguard the personal information of individuals.

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.

Other Holds: Any hold (other than a Legal Hold) that is placed on a Record or a set of Records that supersedes the authority of the Records Retention Schedule.

Personal Information: As defined under FIPPA, personal information means recorded information about an identifiable individual, including:

- 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 the College 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.

Personal information does not include:

- a) the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity;
- b) information about an individual who has been dead for more than thirty years; and,
- c) records of graduation that are otherwise publicly disclosed.

Record: refers to any Record of information however recorded, whether in printed form, on film, by electronic means, handwritten or otherwise (as per FIPPA). Fleming has several Record types and Record stages that are detailed in the charts below. Please note that these examples are intended to provide illustrative examples and is not comprehensive.

Physical Records: are records comprised of any physical medium. This includes correspondence, memos, books, plans, maps, drawings, graphic work, microfilm, sound recordings, videotapes, and any other documentary material.

Electronic Records: are records created and maintained in a digital format or system. This includes email, Word/Excel/PowerPoint documents, databases, text messages, SharePoint and Teams content, social media posts, etc.

Transitory Records: are records only created to move or support the creation of other records, i.e. printing a PowerPoint slide to copy statistics into an Excel spreadsheet. Transitory records do not need to be maintained by retention schedules.

Record Archive: an archival collection made up of historical Records relating to the activities, business dealings, and unique contributions of the College. College Archives chronicle the history of the College from its inception onward, and provides evidence, context, and value to its history; as well as imparting a memory to the College Community.

Records Life Cycle: The process of planning, creating, managing, storing, implementing, protecting, improving, disposing, and preserving of all Records.

Records Retention Schedule (RRS): The formal document which outlines the retention period and whether a record is to be archived or destroyed through the process outlined in OP 1-104.

Retention Period: The specified length of time records should be kept according to their RRS.

Record Security: Refers to the safety of College Records in relation to matters such as access control, authentication, change management and version control, disaster management, effective incident detection, reporting, physical and virtual Security.

User: Any employee or authorized contractor and/or agent who accesses, creates, inputs, amends, deletes, extracts, and/or analyses Records in order to carry out their day-to-day duties.

4.0 - Scope

This policy applies to all college departments, faculty, staff, and contractors who create, manage, or maintain records on behalf of the College. This includes records related to governance, academic delivery, administrative functions, and all other College business.

This policy applies to all Records regardless of their format, and whether they are held on site, or in external locations.

5.0 – General Principles

The College creates records as part of its everyday activities and operational needs. Effective management of these records is critical to meeting legislative, regulatory, contractual and policy obligations – in addition to ensuring effective uses of space, both virtually and physically.

5.1 Record Classification and Access

Records are classified per OP6-604A Information Security Classification – these levels of classification are: Public, Internal, Confidential, Highly Confidential. Where records of multiple classifications are stored together, the repository is classified at the highest level included in the set.

Physical records are to be stored in secured environments to prevent loss, damage or unauthorized access – while also being accessible should the need arise.

Electronic records are to be stored in appropriate systems with controls, backup procedures and disaster recovery measures.

Access is to be granted as appropriate per 1-111 Access to Information and Protection of Privacy, as well as internal needs of confidentiality.

5.2 Ownership and Responsibility

Fleming College is the owner of all Records in its custody, unless subject to an agreement which contradicts this. Appropriate organization, classification, security and management is expected by all levels of the organization.

Records generated on a Device that is the result of an Employee's relationship with the College are considered the property of the College.

The Office of Primary Interest is responsible for the maintenance, security and disposal of all Records that they are responsible for per Retention Schedules and OP 1-104.

5.3 Record Life Cycle

Records are to be securely held based on their classification, until meeting the requirements as laid out in Record Retention Schedules. At which time, the records are to be disposed of following OP 1-104 Record Retention.

Archived records must be maintained with the same security as active records, based on their classification.

Records that are being destroyed must be done so in a manner which ensures the complete destruction or deletion of the record.

6.0 - Related Documents

- *Freedom of Information and Protection of Privacy Act* R.S.O. 1990
- Personal Health Information Protection Act
- OP 6-604A Information Security Classification
- OP 1-104 Record Retention
- 1-111 Access to Information and Protection of Privacy

History of Amendments/Reviews

Date Approved	Approved By	List of Approved Amendments / Review
May 28, 2025	Board of Governors	NEW