FLEMING

Procedure Title:	Record Retention
Procedure ID:	#OP 1-104
Manual Classification:	College Policies
Linked to Policy:	1-104 Record Retention
Approved by Senior Management Team (SMT):	May 28, 2025
Effective Date:	June 1, 2025
Next Review Date:	June 1, 2028
Contact for Procedure Interpretation:	Vice President, Information Technology & Digital Strategy

1.0 – Purpose

This procedure outlines a consistent process for the storage, archiving and destruction of Records in accordance with the associated Record Retention Schedules, and the classification per OP 6-604A

2.0 – 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 retention is met.

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.

Legal Holds: Supersedes all College policies authorizing destruction of Records, including the authority granted in approved retention schedules. Records scheduled for destruction must not be disposed of when such Records are:

a) Relevant to current or foreseeable litigation

b) Responsive to an active request made under FIPPA and/or PHIPA;
c) The subject of an audit; or
d) Relevant to an internal appeal or investigation.

Office of Primary Interest (OPI)/Record Owner: 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 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 charts 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. They may also include copies of records kept outside the Office of Primary Interest.

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 archived or destroyed through the process outlined in OP 1-104.

Retention Period: The specified length of time records should be kept before disposal or archiving.

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-today duties.

3.0 – Guiding Principles

This procedure provides the process by which Records are to be managed throughout their life cycle, from creation to final archiving or destruction.

4.0 – Scope

This procedure applies to all Records created as a part of College operations. All staff members are responsible for assisting in records management, and ensuring records are maintained according to their classification per OP6-604A.

Administrators in the Office of Primary Interest are responsible for ensuring that records are maintained appropriately and that employees are aware of their responsibilities to protect information and provide access where appropriate.

Senior administrative employees hold final accountability that records are maintained according to this procedure and its associated policy.

The Data Governance Committee, appointed by the Chief Technology Officer, is responsible for the oversight and review of governance practices, maintenance, inventories, use, and management of College data, and to provide consultation and guidance to the College regarding data handling practices in the application of relevant College policies, procedures and statutory requirements.

5.0 – Operating Procedure

5.1 Record Owner

Only the Office of Primary Interest, which owns a record, is responsible for maintaining it according to its Retention schedule. All other departments may dispose of transitory copies when they no longer have need of them.

All departments must maintain all records according to their classification, regardless of whether they are the owner.

As an example, the Office of the Registrar is the Office of Primary Interest and thus owner of student application records. If a School Office was given a copy of this record, they may destroy it when it is no longer of use. Until that record is destroyed, the School must maintain it based on its classification, which includes personal information.

5.2 Destruction or Archiving Process

College Records fall into Retention Schedules, which outline the time which a record must be held before it is destroyed or archived. Broad examples are provided in the RRS to show which records belong to which Schedule.

All areas of the College will review their records annually and establish what records that they are the Record Owner (OPI) of may be archived or destroyed. A list is to be created and maintained with the following details:

- Record Series the Records fall under
- A brief list of records being destroyed or archived of
- Date range of the records in question
- Date when these records became eligible for destruction or archiving
- Approval of the administrative employee responsible for OPI
- Date of destruction or archiving

An example template of an list will be provided as a separate document which departments are free to use.

The approver is responsible for confirming that there is no legal or other hold for the destruction and that there is no known operational reason to supersede Retention Schedules and hold the Record.

Legal holds supersede all policies and retention schedules. Other holds can include:

e) Relevant to current or foreseeable litigation
f) Responsive to an active request made under FIPPA and/or PHIPA;
g) The subject of an audit; or
h) Relevant to an internal appeal or investigation.

Departments must maintain their records management list, which can be shared with the Data Governance Committee or Privacy and Policy Officer upon request.

5.3 Methods of Archiving or Destroying Records

Archiving

Records that are to be archived per their RRS may be moved to a secure storage area following approval of their disposition.

These records must continue to be secured based on their classification. While not they do not need to be as readily accessible as actively used records, they still are required to be accessible upon need or request.

Containers for storage are to be labelled, and the list used to track disposition be printed in part where applicable to the container and included for reference of content.

Destruction

Once approved, physical records are to be destroyed by being placed into a secure storage bin for shredding to be collected by the contractor of record. Records can also be destroyed by shredding on site.

Following approval, electronic records are to be deleted from wherever they have been saved, either on hard drives, S Drives, cloud storage, etc.

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
- 1-104 Record Retention
- 1-111 Access to Information and Protection of Privacy

7.0 – History of Amendments & Reviews

New policy 2025.

Date Approved	Approved By	List of Approved Amendments / Review
May 28, 2025	Senior Management Team	NEW