

Complete Policy Title

Records Management Policy

Policy Number (if applicable):

RMM-1001

Approved by

Presidents and Vice Presidents

Date of Most Recent Approval

February 13, 2024

Date of Original Approval(s)

February 13, 2024

Supersedes/Amends Policy dated

Responsible Executive

University Secretary & Privacy Officer

Policy Specific Enquiries

[Privacy Office \(University Secretariat\)](#)

General Policy Enquiries

[Policy \(University Secretariat\)](#)

DISCLAIMER:

If there is a discrepancy between this electronic policy and the approved copy held by the University Secretariat, the approved copy prevails.

FORMAT:

If you require this document in an accessible format, please email policy@mcmaster.ca.

INTRODUCTION

Purpose

1. The purpose of this Policy is to enable McMaster University to manage University Records in compliance with legal requirements and best practices. This purpose includes:
 - a) evaluating and monitoring the creation and use of records, forms, and filing systems;
 - b) ensuring the ongoing identification, management and preservation of records of corporate, fiscal, legal, regulatory, administrative, operational, and historical value;
 - c) supporting the protection of sensitive information by ensuring records are managed and disposed of in an appropriate manner, and in compliance with relevant legislation and policies;
 - d) protecting the University from risks associated with inadvertent or inappropriate destruction of information, and;
 - e) encouraging cost-effectiveness as it relates to records management.

Scope

2. This policy applies to all University Records.

Terms and Definitions

3. For the purpose of interpreting this document:
 - a) Words in the singular may include the plural and words in the plural may include the singular;
 - b) **University Records** are defined as any recorded information, regardless of format or characteristics, that are created or received by an individual in the course of the individual's employment or contract with the University that document university transactions, activities and decisions, including records created or received as a result of research activities. Transitory records do not fall within the scope of this policy. Records in the custody and control of unions, partner institutions, or affiliated organizations do not fall within the scope of university records at McMaster University;
 - c) A **Record Holder** is any individual within the University who has direct custody and/or control of University Records; and

Policy Revision

4. As per the *McMaster University Policy Framework*, the Responsible Executive will normally review this policy every five years. Smaller-scale and more frequent reviews may occur to ensure that this policy is current and compliant with relevant standards and legislation.

PRINCIPLES

5. All University Records, regardless of format or location, are the property of the University.
6. Good records management practice is essential to managing University information throughout the information lifecycle, including its creation, reception, capture, use, and disposition of information required for the University to fulfill its obligations and meet the expectations of its stakeholders.
7. Data, while comprised of information, does not constitute records; However, where the management of data results in a non-structured document (examples include reports or logs), the product would be a record. In addition, Metadata, while not a record, can support the integrity and authenticity of a record.
8. The McMaster Records Management Policy program and practices are based on current professional standards and best practices.

ROLES AND RESPONSIBILITIES

9. The University Secretary and Privacy Officer will provide leadership and strategic management of University Records as essential information assets. They will develop procedures and guidelines to support the implementation of records management best practices. The University Secretariat will provide stakeholders with training and other advisory services to support ongoing collaboration.
10. Senior Unit Leaders (or delegates) are responsible for record management within their unit. They shall ensure that employees who have access to or work with University Records are aware of this policy and are trained appropriately.
11. As Record Holders, all university employees shall effectively manage the University Records within their control and ensure compliance with this policy and related procedures and processes.

RECORDS CREATION AND RETENTION

12. University Records are received and/or created as evidence of University activities and transactions, regardless of format.
13. Employees should consult with their local IT or UTS to determine the appropriate method and location to store digital records.
14. University Records include operational and administrative records created as a result of activities and transactions, and retention in accordance with the function and purpose of the record. The location or format of University Records does not impact the retention requirements.
15. University Records shall be classified and organized appropriately to ensure the information's authenticity, integrity, reliability and security.
16. University Records will be retained in accordance with the *McMaster Records Retention Schedule (MRRS)* to ensure that information is retained only for as long as they are needed, and in compliance with relevant

regulatory, operational, or industry requirements. University Records may be retained beyond the retention requirement, where the information pertains to an ongoing or reasonably anticipated investigation, legal action or proceeding, freedom of information (FIPPA) request for access to information, audit or program review.

17. University Records with archival value shall be identified and preserved in compliance with the *McMaster Records Retention Schedule (MRRS)*.

RECORDS DISPOSITION

18. Records Disposition, which occurs at the end of a Record's retention, may include destruction, archival transfer, or archival selection.
19. Employees must ensure that records are destroyed securely once a retention requirement has been met. The destruction of University Records should be documented for future reference.
20. Record holders responsible for University Records with long-term retention requirements or identified as archival should consult with the University Secretariat to determine long-term preservation strategies to maintain reliable access to the information.

RECORDS ACCESS AND SECURITY

21. Record Holders will maintain appropriate security of University Records to protect the information from inappropriate access, use, disclosure, alteration, and disposal.
22. Requests for access to University Records must be submitted to the Privacy Office in the University Secretariat.
23. University Records may not be removed from the custody and/or control of the University or destroyed except in accordance with this policy. Using personal devices to access, use, or disclose University Records is prohibited without express authorization from the Senior Unit Leader (or delegate).
24. Upon termination, or retirement, from the University, record holders must ensure that all University Records within their control are transferred to the control of the Senior Unit Leader (or delegate).

INFORMATION GOVERNANCE

25. The University Secretary and Privacy Officer shall establish an Information Governance Committee to recommend to the senior administration/President institutional strategic direction and governance of records management policy and processes. The committees will be responsible for evaluating and reviewing records management policies and procedures, including a regular review of the *McMaster Records Retention Schedule (MRRS)*.
26. The committees will consist of stakeholders from across the University community, including senior administration, subject-matter experts, and those with key information and experience to support University Records management practices.

APPENDIX A: DEFINITIONS

Access to information refers to the right granted by FIPPA and other applicable legislation for any person to obtain access to a record of information in the University's custody or control.

Access Control is the permission granted to a University employee to access and use University Records and information within established restrictions of privacy legislation, confidentiality, security clearance and university policies.

Capture is the process of obtaining records (or documents) created in an information management system and recording their existence in the system.

To have **Custody** of a record, the University must have the record in the possession of one of its offices, electronic databases, or filing systems. To have custody of a record, the University must also have the right to manage the record and responsibility for its care and protection.

Disposition is the final action taken once a records retention has been met. These actions include secure destruction or transfer to an archive for a selection process.

A **Document** is recorded information which may constitute a University Record on its own or in relation to a series of documents.

Information Authenticity is the extent to which a record can be proven what it purports to be.

Information Integrity of a record is the quality of being whole and unaltered through loss, tampering, or corruption.

A **Legal or Disposition Hold** is the temporary suspension of the destruction of records that may be relevant for litigation or government investigations.

McMaster Records Retention Schedule (MRRS) is a tool that lists all categories of records produced or maintained by the university, how long they need to be retained, and what the disposition is for each record type.

Metadata is data used to classify electronic records, describe their context, content and structure, and management.

Non-records are information-bearing objects excluded from the scope and authority of the *McMaster Records Retention Schedule (MRRS)*, including reference material, catalogues, and information on non-University business content.

An **Official Record** is the version of a record designated as *original* to satisfy the *McMaster Records Retention Schedules (MRRS)* requirement for information existing in multiple copies.

A **Personal Information Bank (PIB)** refers to a collection of personal information in structured forms that is organized and capable of being retrieved using an individual's name or an identifying number assigned to the individual. Examples include a spreadsheet containing personal information and a database containing personal information.

A **Personal Information Bank (PIB) Directory** is a publication required by the Freedom of Information and Protection of Privacy Act (FIPPA) describing the University systems where the personal information of stakeholders is maintained.

Records include recorded information, regardless of format or characteristics, in any media or format that provides evidence of transactions, activities, and decision-making. University Records, which document transactions, activities, and decision-making at the University, are included within the scope and authority of the *Records Management Policy* and the McMaster Records Retention Schedule (MRRS).

Record Retention is an aspect of records management work that determines how long records must be retained.

A **Record Series** is a group of logically-related records supporting a specific business activity or administrative operation that are filed, indexed, and/or used together.

Records Management is a specialized business discipline concerned with the systematic analysis and control of recorded information.

Information Reliability of a record is the quality of being dependable and worthy of trust.

Information Security includes measures taken to protect materials from unauthorized access, change, destruction, or other threats.

APPENDIX B: RELATED POLICIES AND RESOURCES

- *Freedom of Information and Protection of Privacy Act, 2003* (FIPPA)
- *McMaster University Act, 1976*
- Privacy Management Policy
- [McMaster Records Retention Schedule](#)
- Data Governance Policy
- [Information and Data Classification Policy](#)
- Records Management resources and tools provided to the University community through the University Secretariat website.