Information Management

Purpose

- To manage and protect University Records created in the conduct of University activities in accordance with relevant legislation, University policy, standards, guidelines and procedures;
- To provide a framework for the University's Information Management and Protection Program; and,
- To support information access and privacy and enterprise risk management services throughout the University.

Scope

All Units and all Official and Transitory University Records.

Exclusions:

- Materials acquired for the purpose of creating or augmenting the University's library collections;
- Archival or published materials collected as reference material to support teaching and research programs;
- Personal Health Information that is subject to the *Personal Health Information Act, SNL 2008, C P-7.01, as amended*;
- Teaching materials; and,
- Research data and materials, including unpublished data and manuscripts.

Definitions

Academic Staff Member (ASM) — A Member of the University Community whose terms and conditions of employment are defined in the MUN–MUNFA Collective Agreement.

Artificial Intelligence (AI) – Information technology that performs tasks that would ordinarily require biological brainpower to accomplish, (e.g., making sense of spoken language, learning behaviours, or solving problems). (Source: Government of Canada (GoC)).

ATIPPA – The *Access to Information and Protection of Privacy Act, 2015, SNL 2015, C A-1.2*

ATIPP Request — A request made under the Access to *Information and Protection of Privacy Act, 2015, SNL 2015, C A-1.2*, as amended, for access to a record, including a record containing personal information about the applicant, or correction of personal information.

Cloud — Internet-based computing provided by a third party for computer processing resources and/or data storage.

Important Decision — A decision that has a significant or long-term impact on the high value activities or direction taken by the University in the fulfillment of its mandate.

Information Management — Encompasses records management and refers to the systematic process of creating, using, storing, managing or preserving the University's data, information and records in accordance with this policy, throughout all stages of the information Life Cycle.

Information Management and Protection Lead – A designated employee selected by the Unit Head to oversee operational matters related to the Information Management and Protection Program and to liaise with the OCIO in matters related to implementation of and compliance with the policy.

Information Management and Protection Program — A program of policies, procedures, standards, schedules, guidelines and practices that provides an efficient system for the management and protection of information, in compliance with relevant legislative, regulatory and policy requirements.

Information Asset — An information asset is a collection of recorded information, defined and managed as a unit so it can be understood, shared, protected and used effectively.

Information Risk Assessments — A risk-based approach to classifying University information and identifying the appropriate controls required to ensure the information's confidentiality, integrity and availability throughout its Life Cycle.

Life Cycle — The stages through which information is managed. Information must be managed and protected in a manner that addresses requirements for confidentiality, integrity and availability throughout all Life Cycle stages, including the creation, use, storage, and disposal or preservation of information.

Member of the University Community — An employee or other individual acting at the request of and on behalf of the University.

OCIO — Office of the Chief Information Officer.

Official University Email Account - An account with an email address ending with "mun.ca" (or a Memorial-sanctioned domain) provided to eligible Members of the University Community. This email account may be granted to other individuals and entities who have been identified as requiring email privileges at Memorial University.

Official University Records — University Records created, received or held as evidence of the University's organization, policies, decisions and operations.

Retention and Disposal Schedule — An approved Retention and Disposal Schedule prescribes retention periods and requirements for the legal disposal of Official University Records. It provides direction to ensure that Official University Records are retained for as long as necessary

based on their operational, fiscal, legal and historical value. It also prescribes the appropriate disposition of Official University Records either destruction or preservation.

Transitory University Records — University Records that are of temporary usefulness having no ongoing value beyond an immediate and minor transaction, as convenience copies, or as draft for subsequent University Records. Transitory University Records may be securely disposed of without a Retention and Disposal Schedule.

Unit — Academic or administrative unit, as defined in the University Calendar, or any board or other body appointed or elected to carry out University business.

Unit Head — For the purposes of this policy, unit head is the term used to mean Deans, Department Heads, Division Heads, Heads of Schools, Directors, Executive Directors, University Librarian, University Registrar and other senior administrators at a comparable level; Associate Vice-Presidents and Vice-Presidents, as applicable.

University — Memorial University of Newfoundland.

University Archives — Refers to the archives designated as per *The Rooms Act, SNL 2005, C R-15.1*, as amended, as the repository for Official University Records of archival value.

University Records — All recorded information, regardless of physical characteristics or format. For the purposes of this policy, University Records are categorized as either Transitory University Records or Official University Records.

Policy

1. The University is subject to legislation which relates to its Information Management and Protection Program including: the *Management of Information Act, SNL 2008, C M-1.01, as amended, The Rooms Act, SNL 2005, C R-15.1, as amended,* and the *Information and Protection of Privacy Act, 2015, SNL 2015, C A-1.2, as amended*. The Information Management Policy provides direction for legislative compliance.
2. Information is a vital asset, supporting academic and research excellence, and efficient management of services and resources. Effective management of information enables achievement of the University's strategic objectives by:
    a. increasing transparency and accountability by documenting Important Decisions while protecting the rights and privacy of individuals,
    b. enhancing the efficiency of programs and services,
    c. enabling optimal decision-making and,
    d. managing risk to the University by protecting its Information Assets and ensuring compliance with legislation, University policy, standards, guidelines and procedures.
3. Information management is a shared responsibility:
    a. Members of the University Community are responsible for the University Records they create or that are in their custody.
    b. The OCIO is responsible for the Information Management and Protection Program of the University.
    c. Each Unit Head shall be responsible to ensure adherence to this policy.

    d. Each Unit Head shall designate an Information Management and Protection Lead .
4. University Records are the sole property of the University and must be managed throughout their Life Cycle by Members of the University Community who create or receive them.
    a. University Records must be protected in accordance with the Security Measures section of the Procedure for Administering Privacy Measures within a Unit and the *Electronic Data Security* policy.
    b. Official University Records must be created in a manner and format that is accessible and must be retained only in University-approved repositories as required to support the University's compliance with relevant legislation and policies.
    c. Official University Records may not be removed from the control of the University, destroyed or otherwise disposed of except in accordance with a Retention and Disposal Schedule as outlined in the Procedure for Retention and Disposal Schedules.
    d. Transitory University Records may not be removed from the control of the University, but when no longer required, must be securely disposed in accordance with the Procedure for Secure Disposal of Transitory University Records.
5. The University may use external services, such as commercial record storage and Cloud storage and services, in accordance with related University policy. When considering the use of such external services to store Official University Records, Information Risk Assessments must be completed.
6. An Official University Email Account is provided to eligible Members of the University Community to support the academic and administrative activities of the University. An Official University Email Account is a service that supports the creation and receipt of University Records.
    a. Eligible Members of the University Community, as determined by the CIO and defined here (link), are provided with an Official University Email Account, which they are required to use to conduct all official University email correspondence. A person conducts official University email correspondence where they send or receive emails in the course of their employment with the University, by virtue of their position within the University, or when otherwise acting at the request of or on behalf of the University.
    b. Eligible Members of the University Community are provided with an Official University Email account for the duration of their employment or while acting at the request of and on behalf of the University. Access to the Official University Email Account will be terminated when they are no longer employed or acting at the request of and on behalf of the University.
    c. Information/University Records stored in an Official University Email Account where access is terminated will be retained based on the official email retention schedule found in MUNCLASS.
    d. Notwithstanding Section 6(b), Academic Staff Members, and instructors and research scientists in NAPE 7405 can elect to retain their Official University Email Account upon departure or retirement from the University as defined in the Procedure for Managing Exiting Employees.
    e. Official University Email Accounts are not intended for personal use.

f. The University retains the right to temporarily or permanently disable access to an Official University Email Account for reasons including but not limited to cyber security risks, inappropriate use, and legal requirements.
g. The University reserves the right to access, examine and disclose any information transmitted or stored in an Official University Email Account where the University has reasonable grounds to believe such actions are necessary for safety, security, or operational purposes or to comply with the University's legal obligations.
h. Official University Email Accounts are subject to ATIPPA. The University may be required to provide email correspondence in response to an ATIPP Request. Official University Email Account holders shall comply, promptly and completely, with any request from the University to deliver to the University any records in their custody and control that are potentially responsive to an ATIPP Request.
i. Email sent or received in the conduct of University business is subject to all policies, procedures, guidelines and standards governing University data and information. It is the responsibility of Members of the University Community to retain, manage, dispose and/or archive email in accordance with the MUNCLASS classification and retention plan, and unit directives and practices.

7. Members of the University Community shall not use AI technology with University Records unless it has been approved by the OCIO and is used in compliance with the University's policies and procedures.
8. In the event of any of the following circumstances, disposal of relevant University Records must be suspended:
    a. Notice of litigation or criminal investigation,
    b. Notice of an audit,
    c. Receipt of an ATIPP Request,
    d. When there is reasonable belief that litigation or criminal investigation may occur, and
    e. Initiation of a grievance or investigation pursuant to a University policy or collective agreement.
9. Members of the University Community leaving the University, changing positions within the University, or transitioning from one Unit to another shall manage all University Records in accordance with the Procedure for Managing University Records of Exiting Employees.
10. If, as a result of developing Retention and Disposal Schedules, records are identified as having archival value, they should be transferred to the University Archives.

NON-COMPLIANCE:

Failure to comply with this policy and related procedures may result in prosecution as outlined in Section 8 of the *Management of Information Act, SNL 2008, C M-1.01, as amended*.

Related Documents

Information and Protection of Privacy Act, 2015, SNL 2015, C A-1.2
Electronic Data Security policy
Enterprise Risk Management policy
Information Request policy
Management of Information Act, SNL 2008, C M-1.01

Personal Health Information Act, SNL 2008, C P-7.01
Privacy policy
The Rooms Act, SNL 2005, C R-15.1

Procedure for Managing University Records of Exiting Employees

Units must develop a process to ensure that University Records always remain in the custody and control of the University, and that access to University Records is managed when employees leave positions or transition from one Unit to another. When an employee leaves the University, changes positions within the University, or transitions from one Unit to another within the University the following questions should be answered by the exiting employee:

What University Records in paper format are under your control?

- desktop and desk drawers
- filing cabinets, both in the individual's workspace, shared space or any other location
- records temporarily in the possession of a colleague or another Unit
- commercial records storage

What University Records in electronic format are under your control?

- local hard drive (e.g., C: drive)
- personal drive (e.g., folder on a shared drive only accessible to the individual)
- cloud storage (e.g., OneDrive, Google Drive)
- social media sites managed by the individual on behalf of the University
- Official University Email Account
- calendar accounts
- removable media (USB drives, external hard drives, CDs, etc.)
- devices such as laptops or mobile electronic devices, whether University or personally owned

Once the questions above have been answered and an inventory of University Records has been established, the Unit must ensure that if any University Records are currently not accessible by the University (e.g., on personal DropBox account) they are moved to an accessible location such as a shared drive.

What types of University access do you have?

- University systems such as Banner, OnBase, Memorial’s Incident Management System (MIMS), etc.
- Cloud solutions used for the delivery of University services
- Social media sites managed by the individual on behalf of the University
- Voicemail
- Keys/swipe cards

The Unit Head or Information Management and Protection Lead must ensure the Employee Exit Management process is followed for all exiting employees in their unit.

The Unit Head or Designate must ensure appropriate system and information access is deactivated when an employee transitions from one Unit to another.

In cases where social media sites were being managed by an exiting employee on behalf of the University, the Unit Head or Designate must ensure the individual's account has been deactivated (if it is a named account) or the username and password has been provided to the Unit (if it is a generic University Account). In the case of a generic University account, the password must be changed.

In the case of Cloud solutions being used by an exiting employee for the delivery of University services, it is the Unit Head or Designate's responsibility to terminate any access**.**

Official University Email Accounts

Access to an Official University Email Account will be discontinued upon either the last day of employment or the last day of an individual acting at the request of and on behalf of the University.

Academic Staff Members, and instructors and research scientists in NAPE 7405 can elect to continue to access and use their Official University Email Account upon departure or retirement. They can elect to do so by completing the relevant section of the Termination of Employment Departmental Form completed during the Employee Exit Management process. However, access to an Official University Email Account will be disabled after one year of inactivity and contents purged in accordance with the University's email retention schedule as defined by MUNCLASS.

Employees who departed or retired before <date> and who are currently accessing their Official University Email Account can continue to access their Official University Email Account. However, access will be disabled after one year of inactivity and contents purged in accordance with the University's email retention schedule as defined by MUNCLASS.