Information Management

Authority:

Vice-President (Administration Finance and Advancement)

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- Research data and materials, including unpublished data and manuscripts.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

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 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 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.

~~2.~~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 to oversee operational matters and to liaise with the OCIO in matters related to implementation of and compliance with the policy.

~~3.~~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.

~~4.~~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.

~~5.~~6. 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.

~~6.~~7. 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.

~~7.~~8. 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