Policies, Procedures and Guidelines

Complete Policy Title

Privacy Management Policy

Policy Number (if applicable):

PMM-1001

Approved by

President and Vice Presidents

Date of Most Recent Approval

February 13, 2024

Date of Original Approval(s)

February 13, 2024

Supersedes/Amends Policy dated

- Policy for the Handling of Personal Health Information, June 16, 2015 *(Approved by President)*
- Policy for the Handling of Personal Information, June 16, 2015 *(Approved by President)*
- Policy Governance and Accountability Framework, June 16, 2015 *(Approved by President)*

Responsible Executive

University Secretary and 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.*

TABLE OF CONTENTS

SECTION I: INTRODUCTION

PURPOSE

1. The purpose of this policy is to:

    a) establish the roles and responsibilities of McMaster University regarding the protection of privacy and the right of access to information in compliance with privacy laws, specifically the *Freedom of Information and Protection of Privacy Act (FIPPA), RSO, 1990* and the *Protection of Personal Health Information Protection Act (PHIPA) S.O., 2004*;

    b) ensure that personal information in the University's custody and control, including personal information that has been received by the University through an agent or services provider, is managed and protected in accordance with FIPPA, PHIPA and other applicable legislation; and

    c) provide principles and accountability mechanisms to ensure that all McMaster Employees involved in the planning, management and day-to-day operations of the University are in compliance with FIPPA and with PHIPA, their associated regulations and the privacy policies, procedures and practices set out by the University.

SCOPE

2. This policy applies to all Personal Information created, received, used, and retained in the custody and control of University employees.

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) **Assignment Employees** are individuals employed by a temporary help agency and assigned to perform work on a temporary basis for the University;

    c) **Employees** include only those individuals who are considered employees of the University under the *Employment Standards Act*, 2000 (the "Employment Standards Act"). This includes faculty, staff, members of the Management Group (TMG), postdoctoral fellows, sessional faculty, teaching and research assistants, clinical faculty, librarians, employees who are members of a bargaining unit, and interim employees. It also includes employees in supervisor roles (e.g., directors, chairs, deans).

    d) **Personal Health Information (PHI)** is identifying information about an individual, in oral or recorded form, if that information relates to the physical or mental health of the individual and relates to the provision of healthcare to the individual or includes the individual's health card number;

e) **Personal Information (PI)** is recorded information about an identifiable individual. Personal Information does not include Business Identity Information;[1] and

f) **University Records** are defined as any recorded information, regardless of format or characteristics, in any media or format, within the University's custody or under its control. University Records may be created or received and maintained as information or evidence in the administration and operation of the activities of the University.

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.

[1] Resources regarding the sharing of personal information is available on the privacy office website.

SECTION II: PRINCIPLES

5. Records, as prescribed by FIPPA, will be available to members of the University community and to the public subject to specific and limited exemptions. To facilitate access, the University will describe University records containing personal information in its directory of personal information banks.

6. The collection, use, disclosure, retention and disposal of personal information contained in University records will be regulated in accordance with FIPPA and other applicable legislation to support the protection of the privacy of individuals who are the subject of that information.

7. Consistent with its commitment to accountability and transparency, the University actively publishes information about its operations, activities, policies, practices and procedures. Information derived from personal information will be published in aggregate form and anonymized.

SECTION III: ROLES AND RESPONSIBILITIES

8. The accountability for ensuring that entities and individuals associated with the University comply with FIPPA and PHIPA, and all relevant regulations, policies, procedures, and guidelines is distributed as follows:

Role	Accountability	Responsibility
Privacy Officer (University Secretariat)	President	Duties including but not limited to: • provide guidance and tools to support the appropriate management of personal information in the University's custody and/or control is collected, used and disclosed in accordance with FIPPA and/or PHIPA and with University policy; • ensure that relevant information and training to support compliance and privacy best practices is available to faculty, staff and students; • submit an annual privacy report in respect of the University's operations in compliance with the FIPPA for submission to the Information and Privacy Commissioner's (IPC) Office of Ontario; • assess agreements, processes and practices, including those with external vendors, to ensure provisions supporting compliance.
Chief Operating Officer (FHS)	Dean and Vice-President, Faculty of Health Sciences	Duties including but not limited to: • work in partnership with the University privacy office to assess and review practices and processes periodically to support compliance with FIPPA and/or PHIPA; • ensure that Employees, Assignment Employees, contracted workers, volunteers, students and vendors in the Faculty of Health Sciences who have access to PHI in their work have the tools and support necessary to comply with PHIPA and relevant policies, procedures, and practices of the University;

		• ensure in written agreements with affiliated organizations that their agents similarly comply with relevant legislation and policies, procedures and practices of the University.
Health Information Custodians (HIC)	McMaster University	Duties including but not limited to: • **w**ork in partnership with the University privacy office to assess and review practices and processes periodically to support compliance with FIPPA and/or PHIPA; • provide supervision for agents, as delegated by HICs, in managing PI and PHI; • collect, use, access, disclose, retain, alter, correct, or destroy information that includes personal health information, in compliance with the legislation and this policy.
All University Employees, student workers, contract-based workers, and service providers associated with the University	McMaster University	Duties including but not limited to: • ensure a strong understanding of privacy compliance requirements and manage information in their custody and control appropriately; • complete mandatory privacy training; • be familiar with the University privacy incident protocol and report all privacy incidents to their supervisor and the privacy office.
Volunteers who have access to Personal Information at the University, including members of the Board of Governors and the Senate	McMaster University	Duties including but not limited to: • ensure a strong understanding of privacy compliance requirements and manage information in their custody and control appropriately; • recommended privacy training; • be familiar with the University privacy incident protocol and report all privacy incidents to their supervisor and the privacy office.

SECTION IV: COLLECTION AND USE OF PERSONAL INFORMATION

9. University offices may collect and use personal and personal health information for the following purposes:

    a) for the specific purpose that an individual originally provided the information to the University;

    b) to provide individuals with University services, relevant to their role(s);

    c) as a basis for planning and providing support services;

    d) for the development, delivery, and supervision of programs and services by the University;

    e) to support continuous improvement and evaluation of University services; and

    f) to process financial transactions.

10. All reasonable steps will be taken to ensure that Consent is informed and voluntary.

11. The University will publish a *Statement on Collection, Use, and Disclosure of Personal Information* outlining the general purposes for the collection and use of personal information in compliance with FIPPA.

12. In specific circumstances, the University may be required to collect, use or disclose personal information without an individual's expressed consent in the course of duties or as required by law.(See *also § VII.18*)..

SECTION V: INFORMATION ACCESS AND CORRECTION

13. Individuals have a right of access and correction to records in the custody or control of the University unless:

    a) a record or part of the record falls under one of the exemptions identified in FIPPA (see *Appendix B: Exemptions and Exclusions to Access to Information*);

    b) the University has reasonable grounds to determine that a request for access is frivolous or vexatious.

14. A statement of disagreement will be attached to the personal information reflecting any correction that was requested but not made.

SECTION VI: PROTECTION OF PRIVACY

15. Records containing personal or personal health information must be classified as restricted in compliance with the *Information and Data Classification Policy*.

16. University offices who have the custody and/or control of records containing personal or personal health information shall ensure that such information:

    a) is appropriately secured and protected from unauthorized access, use, revision, and destruction;

    b) is only accessible to University staff who are authorized for such access and use;

    c) remains in the custody and control of the University;

    d) is regularly reviewed, and access and permissions are updated as needed.

SECTION VII: DISCLOSURE OF PERSONAL INFORMATION

17. University offices who have the custody and/or control of records containing personal or personal health information must ensure consent has been obtained prior to disclosing such information.

18. In specific circumstances, the University may disclose personal or personal health information without the consent of the individual. These circumstances include:

    a) when the individual's actions pose a risk of health and safety to themselves or others;

    b) where disclosure is made to an officer, Employee, consultant or agent of the University who needs the record in the performance of their duties and where disclosure is necessary and proper in the discharge of the University's functions;

    c) where permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada;

    d) to an institution or a law enforcement agency in Canada if,

        (i) the disclosure is to aid in an investigation undertaken by the institution or the agency with a view to a law enforcement proceeding, or

        (ii) there is a reasonable basis to believe that an offence may have been committed, and the disclosure is to enable the institution or the agency to determine whether to conduct such an investigation;

    e) in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill, or deceased;

    f) to a member of the bargaining agent who has been authorized by an Employee to whom the information relates to make an inquiry on the Employee's behalf or, where the Employee is incapacitated, has been authorized by the spouse, a close relative or the legal representative of the Employee;

    g) to the Information and Privacy Commissioner;

    h) to alumni administration, for the purpose of fundraising activities or the fundraising activities of an affiliated foundation, if the personal information is reasonably necessary for the fundraising activities.

19. Any unauthorized use, loss of record, disclosure, or disposal will be reported to the University privacy office for investigation.

SECTION VIII: RECORDS STORAGE, RETENTION AND DISPOSAL

20. Personal and personal health information may be stored in any format.

21. An individual's personal information will be retained for a minimum of one year after use, in compliance with *FIPPA*. Personal information may be retained for a shorter period if consented to by the individual(s) at the time of collection. Thereafter the personal information will be disposed of in accordance with the *McMaster Records Retention Schedule (MRRS)*.

22. Care must be taken in the disposal or destruction of records containing personal or personal health information to prevent early destruction or unauthorized access to the information.

23. When records are destroyed or deleted, all reasonable steps will be taken to ensure the information cannot be retrieved, or identifiable.

APPENDIX A: GLOSSARY

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 that is in the University's custody or under its control.

An **Agent** is a person, with the authorization of the University, acting for or on behalf of the University for the purposes of the University and not the agent's own purposes, whether the agent has the authority to bind the University, whether the agent is employed by the University and whether the agent is being remunerated. For the purposes of this policy, a consultant is an agent.

In the context of Privacy Management, **Consent** is given either verbally or in writing, to a custodian to collect, use or disclose your personal information. Students and University Employees provide implied consent in regard to the University's Notice of Collection, Use, and Disclosure Statement.

University offices may have **Control** of a record, even if a record is not in their direct custody. For example, if an office has the authority to manage a record related to a University mandate and function and staff rely on it for business purposes, it may be under the University's control regardless of whether the record is stored by or at the University. A record held by a consultant, for example, could be considered in the University's control in some circumstances.

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.

Information and Data Classification refers to the University's classification levels for data and information to ensure the level of information protection and privacy is commensurate with the sensitivity and value of that data.

A **Privacy Incident** occurs when an unauthorized individual gains access to personal information, either in error, or through mischief.

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 of this include a spreadsheet containing personal information, and a database containing personal information.

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)*.

A **Privacy Impact Assessment (PIA**) is an organizational risk management process used to identify the effects of a given process or other activity on an individual's privacy. This is often done in conjunction with an information security assessment.

APPENDIX B: EXEMPTIONS AND EXCLUSIONS TO ACCESS TO INFORMATION

Section	Exemptions	Type of Exemption	Public Interest Override (s.23)
10	Frivolous and Vexatious Request	Discretionary	No
12	Cabinet Records	Mandatory	No
13	Advice to Government	Discretionary	Yes
14	Law Enforcement	Discretionary	No
14.1	Remedies for Organized Crime	Discretionary	No
14.2	Prohibiting Profiting from Crime	Discretionary	No
15	Relations with other Government	Discretionary	Yes
16	Defence	Discretionary	No
17	Third-Party Information	Mandatory	Yes
18	Economic & Other Interests of Ontario	Discretionary	Yes
18.1	Closed Meetings	Discretionary	No
19	Solicitor-Client Privilege	Discretionary	No
20	Danger to Safety or Health	Discretionary	Yes
21	Personal Privacy	Mandatory	Yes
21.1	Fish and Wildlife Species at Risk	Discretionary	Yes
22	Published Information	Discretionary	No
49	Personal Information	Discretionary	No

Exclusions

The Act does not apply to the following categories of information, and as a result may not be disclosed in response to an access to information request.

65(6)2	Negotiations or anticipated negotiations relating to labour relations or to the employment of a person by the institution between the institution and a person, bargaining agent or party to a proceeding or an anticipated proceeding.
65(6)3	Meetings, consultations, discussions or communications about labour relations or employment-related matters in which the institution has an interest.
65(8.1)	(a)to a record respecting or associated with research conducted or proposed by an employee of an educational institution or by a person associated with an educational institution (b)to a record of teaching materials collected, prepared or maintained by an employee of an educational institution or by a person associated with an educational institution for use at the educational institution.
67(2)	Confidentiality Provisions in Other Acts (which prevail over FIPPA)

APPENDIX C: RELATED POLICIES AND LEGISLATION

This Policy is to be read in conjunction with the following policies, statements, and collective agreements. Any question about the application of this Policy or related policies shall be determined by the President or University Secretary, as appropriate, and in conjunction with the administrator of the other policy or policies. Normally the policies listed below act independently of one another. However, they may intersect with the application of other University policies or procedures regarding the same matter. The University reserves the right to amend or add to the University's policies and statements from time to time (this is not a comprehensive list):

- *Freedom of Information and Protection of Privacy Act, 2003* (FIPPA)
- *Information and Data Classification Policy*
- *McMaster University Act, 1976*
- McMaster University Statement on Collection, Use, and Disclosure of Personal Information
- *Personal Health Information Protection Act, 2004* (PHIPA)
- *McMaster Records Retention Schedule (MRRS)*
- Records Management Policy
- Privacy Management resources and tools provided to the University community through the University Secretariat website.