MacEwan UNIVERSITY
PRIVACY AND INFORMATION MANAGEMENT

PRIVACY MANAGEMENT PROGRAM

MacEwan University

June 2026

Prepared by:
Information and Privacy Office
Office of General Counsel

In accordance with the
Protection of Privacy Act (Alberta)

Table of Contents

Purpose:
This Privacy Management Program establishes MacEwan University's governance, policies, safeguards, training, monitoring, and transparency commitments required under the *Protection of Privacy Act (POPA), Protection of Privacy Regulation* and the *Protection of Privacy (Ministerial) Regulation*. **Link to the Protection and Privacy Act**

1. Governance and Accountability

1.1 Designated Privacy Officer

MacEwan University designates a **University Privacy Officer** within the Office of General Counsel / Information and Privacy Office.

The University Privacy Officer is responsible for administering the Privacy Management Program and supporting compliance with applicable privacy legislation, including oversight of Privacy Impact Assessments (PIAs), breach response management, and privacy risk mitigation activities.

The University Privacy Officer serves as the University's primary point of contact for privacy matters and provides advice, guidance, and oversight to faculties, departments, and administrative units on the collection, use, disclosure, and protection of personal information.

Responsibilities of the University Privacy Officer include:

- providing strategic and operational privacy advice;
- overseeing the development, maintenance, and implementation of privacy policies, procedures, and standards;
- supporting and reviewing PIAs and information sharing arrangements;
- overseeing privacy breach response and notification requirements;
- monitoring compliance with privacy legislation and this Privacy Management Program;
- promoting privacy awareness and training across the University; and
- reporting on the University's privacy posture, risks, and compliance activities to senior leadership.

The University Privacy Officer is supported by institutional partners, including Information Technology Services, Risk Management, and other administrative units, to ensure coordinated implementation of privacy and information protection practices.

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(a).

1.2 Internal Privacy Governance Structure

MacEwan University maintains an internal privacy governance structure that ensures accountability, senior-level oversight, and escalation of privacy risks appropriate to the volume and sensitivity of personal information under its control. Overall accountability for privacy compliance rests with the Head of the Public Body, with specific authorities delegated through a formal Delegation of Authority.

The University Privacy Officer provides an annual privacy report to the Board of Governors outlining privacy breaches, trends, PIAs, and key risk management activities. Privacy-related non-compliance, including breaches and significant compliance issues, is reported through the University's Audit and Risk governance processes, including mitigation measures and assessments of institutional risk exposure. Privacy risks are escalated based on their nature and severity and are considered within the University's broader institutional risk management and governance processes.

Where appropriate, cross-functional collaboration supports the management of privacy risks, including coordination between legal, privacy, information security, and risk management functions.

The University is developing and maintaining personal information banks to support the identification, classification, and management of personal information holdings in accordance with legislative requirements.

Required under the Protection of Privacy Ministerial Regulation, s. 6(2)(a).

2. Policies and Procedures

MacEwan University's privacy-related policies and procedures are available through the University's policy framework:

https://www.macewan.ca/about-macewan/policies/current-policies/policies-current-administrative/#Legal

2.1 Correction Requests

MacEwan University maintains procedures enabling individuals to request correction of their personal information. Requests may be submitted through the Information and Privacy Office, using the available forms:
https://www.macewan.ca/about-macewan/administration/information-and-privacy-office/forms/

Internal procedures and tracking mechanisms support the processing and response to correction requests.

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(b)(i)(A).

2.2 Privacy Breach Response

MacEwan University maintains a privacy breach response protocol that addresses identification and containment of incidents, assessment using the real risk of significant harm criteria, notification to affected individuals and regulators where required, and documentation of breach events.

Breach response activities include assessment of the sensitivity of the information, the likelihood of misuse, and whether there is a real risk of significant harm, as well as post-incident review to support continuous improvement.

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(b)(i)(B) and 4.

2.3 Privacy Complaint Handling

MacEwan University maintains procedures to receive, investigate, and respond to privacy complaints and to inform complainants of outcomes.

Complaints may be submitted through the Information and Privacy Office using the available forms: https://www.macewan.ca/about-macewan/administration/information-and-privacy-office/forms/

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(b)(i)(C).

2.4 Non-Personal Data Management

MacEwan University addresses the use of non-personal data, including data derived from personal information, through its privacy policies and procedures, information technology practices, and institutional data and analysis functions. Where applicable, de-identification practices and consideration of re-identification risk are applied in accordance with legislative requirements and emerging guidance. Additional guidance to support the use and management of non-personal data will be developed and maintained.

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(b)(ii).

2.5 Automated/AI Systems

Where automated tools or systems involving personal information are used, MacEwan University addresses transparency, appropriate safeguards, human oversight, and validation to mitigate risks associated with automated decision-making.

Guidance on the use of artificial intelligence is available through institutional resources, including: https://www.macewan.ca/c/documents/ai-best-practices-guidelines.pdf

PIAs and internal review processes support oversight of automated systems.

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(b)(iii).

2.6 Consent Management

MacEwan University addresses consent requirements through the Information and Privacy Office, including through privacy consultations, application of the *POPA* and associated regulations, and the University's Access and Protection of Privacy policies and procedures.

Consent practices are applied in a manner consistent with legislative requirements, including ensuring that consent is meaningful, informed, and appropriate to the context of the personal information involved.

Guidance on consent may also be informed by provincial resources, including: https://www.alberta.ca/system/files/ti-consent-for-use-or-disclosure.pdf

Required under the Protection of Privacy Ministerial Regulation, s. 6(2)(a)(iv).

2.7 Service Provider and Third-Party Privacy Governance

MacEwan University remains accountable for personal information in its custody or under its control, including where personal information is collected, used, stored, or accessed by service providers. Third-party engagements involving personal information are governed through existing University contracting, procurement, information security, and privacy policies and procedures. Privacy risks associated with third-party services are assessed through PIAs or other risk assessment processes where applicable, and privacy incidents involving service providers are managed in accordance with the University's privacy breach response procedures.

Required under the Protection of Privacy Ministerial Regulation, s. 6(2)(a).

3. Information Classification and Security Safeguards

3.1 University-Wide Information Classification and Security Safeguards

MacEwan University maintains an information classification framework that applies to personal information, data derived from personal information, and non-personal data. Information is classified based on sensitivity and risk, and the classification determines the appropriate safeguards.

MacEwan's Information Classification Levels

Classification	Sensitivity Level
Restricted	Access is strictly limited to authorized individuals. The information is highly sensitive and could cause major risk and harm to the University or individual(s) if breached.
Confidential	Access is restricted by role-based access. The information includes sensitive elements and could cause high risk and harm to the University or individual(s) if

	breached.
Internal	Access is intended for those who are employed, enrolled, or are stakeholders of the University. The information is for the University's internal operations and could cause minor risk and harm to the University or individual(s) if breached.
Public	Access is available for everyone's use and could cause negligible risk and harm to the University or individual(s) if breached.

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(c).

3.2 Administrative, Physical, and Technical Safeguards

MacEwan University implements administrative, physical, and technical safeguards that are proportionate to the sensitivity and classification of personal information, data derived from personal information, and non-personal information.

Administrative safeguards are established through privacy policies and procedures governing the collection, use, disclosure, retention, and protection of information.

Physical safeguards are implemented through institutional practices that control access to facilities, equipment, and systems containing personal information.

Technical safeguards are implemented through information security and information protection controls, supported by Information Technology Services, to protect systems and information from unauthorized access, use, disclosure, or loss.

These safeguards are supported through institutional policies and frameworks, including administrative policies relating to information and security:

https://www.macewan.ca/about-macewan/policies/current-policies/policies-current-administrative/#Information

Detailed technical controls, standards, and operational procedures are maintained internally and are not publicly disclosed.

Required under the Protection of Privacy Ministerial Regulation, s. 6(2)(b).

3.3 Safeguard Oversight and Monitoring

Safeguards are subject to oversight and review through existing governance, risk management, and compliance processes. This may include monitoring activities, reviews of incidents and breaches, and assessments conducted as part of PIAs or other risk evaluation processes. Identified risks

inform corrective actions, mitigation strategies, and continuous improvement of safeguards and controls.

Monitoring activities are proportionate to the sensitivity and volume of information and may include reviews of access controls, incident trends, and compliance with institutional policies.

Based on the Protection of Privacy Ministerial Regulation, s. 6(2)(a)(iii).

4. Employee Training and Awareness

4.1 Mandatory Privacy Training Program

MacEwan University requires all individuals acting on its behalf, including employees, academic staff, and contractors who collect, use, or disclose personal information, to complete mandatory privacy training covering recognition of personal information, collection requirements, authorized use and disclosure, safeguarding practices, breach identification and reporting, and access to information responsibilities.

Additional or role-specific training may be provided to individuals with elevated access to personal information or increased privacy risk responsibilities.

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(d).

4.2 Training Renewal Schedule

MacEwan University requires mandatory privacy training renewal annually and maintains institutional records of training completion.

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(d).

5. Monitoring, Review, and Continuous Improvement

5.1 PMP Review and Update Cycle

MacEwan University reviews and updates this Privacy Management Program on a regular basis (at a minimum, annually) and following significant changes to programs or services, material privacy incidents, or legislative or regulatory developments.

Required under the Protection of Privacy Ministerial Regulation, s. 6(1)(e).

5.2 Internal Audits and Performance Measures

Privacy compliance is monitored through existing governance, risk, and accountability processes.

Monitoring may include the use of performance indicators such as:

- completion of PIAs,

- privacy training participation,
- breach trends and root causes, and
- compliance issues or audit findings.

Findings inform corrective actions and risk mitigation.

Based on the Protection of Privacy Ministerial Regulation, s. 6(1)(e).

5.3 Integration with Risk Management

Privacy risks are considered within the University's broader institutional risk management and governance processes. Information arising from monitoring activities, incidents, and assessments informs governance reporting and ongoing improvements to privacy controls.

6. Privacy Impact Assessments (PIAs)

MacEwan University maintains procedures to ensure PIAs are completed for new or significantly changed programs, services, or systems involving personal information.

Governed by the Protection of Privacy Ministerial Regulation, s. 7.

7. Transparency and Public Access to the PMP

7.1 Public Availability

MacEwan University makes this Privacy Management Program available upon request.

Required under the Protection of Privacy Ministerial Regulation, s. 6(3).

7.2 Removal of Sensitive Details

For public availability purposes, details that could compromise security or increase risk to the University are excluded.

Permitted under the Protection of Privacy Ministerial Regulation, s. 6(4).

8. Appendices

Appendix A — Definitions

Appendix A — Definitions

Purpose of this Appendix
This appendix defines key terms used throughout the Privacy Management Program to ensure a shared and consistent understanding across the University. Where appropriate, definitions align with terminology used in the *Protection of Privacy Act (POPA)* and associated regulations, and are written for clarity rather than legal interpretation.

Definitions

Personal Information

Recorded information about an identifiable individual, including information that can reasonably be used, alone or in combination with other information, to identify the individual.

Data Derived from Personal Information

Information that results from the analysis, aggregation, or transformation of personal information, and that may still present privacy risks depending on context, use, or re-identification potential.

Non-Personal Data

Data that has been modified so that it does not identify an individual and cannot reasonably be used to re-identify an individual, either alone or when combined with other available information.

Privacy Breach

The loss of, unauthorized access to, or unauthorized disclosure of personal information, whether intentional or unintentional.

Significant Harm

Harm that may result from a privacy breach, including bodily harm, humiliation, damage to reputation or relationships, loss of employment or professional opportunities, financial loss, identity theft, negative effects on credit records, or damage to or loss of property.

Real Risk of Significant Harm

A determination that significant harm is more than merely possible following a privacy breach, taking into account factors such as the sensitivity of the personal information and the probability that it has been, or will be, misused.

Privacy Impact Assessment (PIA)

A structured process used to identify, assess, and mitigate privacy risks associated with a new or significantly changed program, activity, or system involving personal information.

Automated Decision System

A system or process that uses automated tools, algorithms, or rules to assist in, or make, decisions that involve personal information, with limited or no human intervention.

Service Provider

An external individual or organization that collects, uses, stores, processes, or accesses personal information on behalf of MacEwan University under an agreement or arrangement.

Safeguards

Administrative, physical, and technical measures implemented to protect personal information, data derived from personal information, and non-personal data against unauthorized access, use, disclosure, modification, or destruction.

Information Classification

The categorization of information based on its sensitivity and risk, used to determine appropriate safeguards and handling requirements.

University Privacy Officer

The individual designated by MacEwan University to administer the Privacy Management Program and oversee privacy compliance, advice, assessments, and incident response.

Use of Definitions

These definitions apply throughout the Privacy Management Program and its appendices. Where terms are defined in legislation, this appendix is intended to support operational understanding and does not replace statutory interpretation.