1.0 ASSOCIATED POLICY

- Privacy Policy

2.0 DEFINITIONS

Office of Record
The University department or business unit that is responsible for maintaining a University record.

Personal Information
Recorded information about an identifiable individual as defined under the FOIP Act, which includes but is not limited to an individual's name, age, ID number, ethnic origin, financial information, biometric information, medical history, or an opinion about the individual.

Record
Recorded information in any form, which includes any notes, images, audio-visual recordings, documents, videos, text messages, social media posts, and any other information that is written, photographed, recorded or stored in any manner but does not include software or any mechanism that produces records.

3.0 PROCEDURE ELEMENTS

3.1 Collection of Personal Information

3.1.1 MacEwan University collects Personal Information under the authority of the Post Secondary Learning Act and in accordance with the FOIP Act to administer its statutory requirements, programs, and activities.

3.1.2 Before collecting Personal Information directly from an individual, University Members must provide a collection notice stating the purpose of collection and how the information will be used.

3.1.3 When Personal Information is to be used or disclosed in a manner inconsistent with the reason for which the information was initially collected, individuals will be asked for their consent.

3.1.4 The FOIP Act allows for indirect collection with consent, in emergencies, for legal services, personnel management, and other limited circumstances permitted under the FOIP Act.

3.2 Use and Disclosure of Personal Information

3.2.1 Personal Information must only be used or disclosed for its intended purpose, with consent or as permitted by law. Use and disclosure should be restricted to what is necessary for the University to accomplish its purpose.

3.2.2 The University may disclose personal information without an individual's consent or original purpose for collection in limited and specific circumstances as permitted under the FOIP Act. This includes the risk of harm to health or safety, assisting law enforcement, fundraising related to post-secondary education, teaching and course evaluations, research purposes, and the University Archives.

3.3 Disclosure in the Public Interest

3.3.1 With the advice from the Information and Privacy Office and the Office of Record, the University is required to disclose any information regarding a considerable threat to the environment, public health, or safety that may affect a group of individuals or a single person, if it is in the public interest.

3.3.2 When disclosing Personal Information in the public interest, the University must disclose only the minimum amount of Personal Information required.

3.3.3 If it is practical, a notification should be given to the affected third party and Alberta's Information and Privacy Commissioner before releasing any information related to them in the public interest. However, the University should ensure that no delay occurs that might harm the public interest.

3.3.4 When advance notification is not possible, written notification must be given to both the affected third parties and Alberta's Information and Privacy Commissioner following the public interest disclosure.

3.4 Protection of Personal Information

3.4.1 To ensure the privacy and security of Personal Information, the University will implement a comprehensive set of measures that includes administrative, physical, and technical controls, including:

3.4.1.1 The University will establish controls in accordance with its Information Security Policy and Information Security Framework Standard. This includes making sure that electronic personal information is only accessible to authorized personnel through proper authentication and access control measures. The use of passwords and encryption, as well as secure servers, firewalls, and anti-malware software, will also be implemented to strengthen the security of the data;

3.4.1.2 providing regular privacy awareness training to educate faculty and staff on data protection principles and responsibilities;

3.4.1.3 ensuring that any Personal Information collected, used, or disclosed by academic researchers is non-identifiable once combined with other information;

3.4.1.4 having information-sharing agreements with standard security safeguards and confidentiality provisions in place before allowing access to Personal Information to third parties;

3.4.1.5 completing Privacy and Security Assessments when considering new technologies or programs involving Personal Information;

3.4.1.6 regularly auditing user activity of electronic information systems that contain Personal Information; and

3.4.1.7 limiting physical access to Records, including the use of locked filing cabinets to contain personal information to prevent unauthorized handling, and limiting access to specific areas within the University.

4.0 RELATED POLICIES, PROCEDURES, FORMS AND OTHER DOCUMENTS

- Access to Information Procedure
- Correction of Personal Information Procedure
- Records Retention and Destruction Procedure
- Use of Personal Information for Academic Research and Creative Activity Procedure

5.0 ACCOUNTABILITY

Responsible Office
Information and Privacy Office

6.0 HISTORY

Relevant Dates

Approved: **2024.08.27**

Effective: **2024.08.27**

Next Review: **2029.08**

Modification History

24.08.27: New procedure. Approved by President's Policy Committee (#2024.08.27-03.3 EC).