

1.0 POLICY STATEMENT

MacEwan University (“University”) is committed to protecting the privacy and confidentiality of personal information that is in its custody or under its control. Toward achieving this objective, the collection, use, disclosure, retention and disposition of personal information will adhere strictly to the provisions of Alberta’s *Freedom of Information and Protection of Privacy Act* (“FOIP Act”) and the *Freedom of Information and Protection of Privacy Regulation* (“Regulation”), and this policy.

2.0 GUIDING PRINCIPLES

- 2.1 The mandate of the University necessitates the collection, use, disclosure, retention, and disposition of personal information of students, faculty, staff, alumni, volunteers, retirees and other individuals. In accordance with the terms of this policy, the FOIP Act and any applicable enactment of Alberta or Canada, the University will take appropriate physical and administrative measures to ensure the confidentiality of personal information that is in its custody or under its control.
- 2.2 The University will act in an accountable and transparent manner when responding to access requests for personal information. Access requests will be viewed objectively in terms of the University’s obligations to the public and under the FOIP Act and will be processed according to the Access to Records and Correction of Personal Information Procedure.
- 2.3 The University’s commitment to complying with the FOIP Act in the conduct of its operations and programs will be achieved by adhering to this policy and associated procedures.

3.0 SCOPE

This policy applies to all members of the University community.

4.0 DEFINITIONS

- 4.1 “authorized persons” means members of the University community who, by virtue of their duties and responsibilities, may collect, use and disclose personal information;
- 4.2 “indirect collection” means the collection of personal information from an individual other than the subject of the personal information;

-
- 4.3 “members of the University community” means those persons involved in conducting University affairs or operations or using University property, including all employees, agents, contractors and volunteers;
- 4.4 “office of record” means the University department or business unit that is responsible for maintaining a University record;
- 4.5 “personal information” means recorded information about an identifiable individual, including
- (i) the individual’s name, home or business address or home or business telephone number,
 - (ii) the individual’s race, national or ethnic origin, colour or religious or political beliefs or associations,
 - (iii) the individual’s age, sex, marital status or family status,
 - (iv) an identifying number, symbol or other particular assigned to the individual,
 - (v) the individual’s fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
 - (vi) information about the individual’s health and health care history, including information about a physical or mental disability,
 - (vii) information about the individual’s educational, financial, employment or criminal history, including criminal records where a pardon has been given,
 - (viii) anyone else’s opinion about the individual, and
 - (ix) the individual’s personal views or opinions, except if they are about someone else.
- 4.6 “personal information collection notice” means a statement that is provided, either in writing or orally, to an individual from whom the University collects personal information and which sets out the
- (i) purpose for which the personal information is collected,
 - (ii) specific legal authority for the collection, and
 - (iii) business address and business telephone number of the head of the privacy department who is able to answer the individual’s questions about the collection.
- 4.7 “privacy department” means the Privacy and Information Management Department;
- 4.8 “record” means a record of information in any form and includes notes, images, audio-visual recordings, x-rays, books, documents, maps, drawings, photographs,

letters, vouchers and papers 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;

4.9 “research information” means the records of facts and ideas that are used by a researcher to conduct an academic inquiry or investigation with the intention of peer dissemination, including but not limited to the following research-related records and information:

- (i) laboratory notebooks,
- (ii) survey documents,
- (iii) questionnaires,
- (iv) interview notes,
- (v) transcripts,
- (vi) machine-generated data or performance outputs,
- (vii) research-subject recruitment materials,
- (viii) consent forms,
- (ix) correspondence and other documents,
- (x) computer files,
- (xi) audio or video recordings,
- (xii) photographs, including negatives, slides, and x-ray films,
- (xiii) permits,
- (xiv) samples of compounds, and
- (xv) components of research organisms;

4.10 “routine disclosure” means the granting of access to a record of non-personal information, usually in response to a routine inquiry or request, without the submission of an access request under the FOIP Act;

4.11 “teaching materials” mean a record of facts, information, or ideas that an instructor uses to prepare for or engage in academic teaching, including course materials, course content, teaching methodology and a record of communication between two or more instructors regarding course content, materials and teaching methodology, but does not include correspondence regarding a specific student or students or correspondence between an instructor and a student.

5.0 REGULATIONS

5.1 Collection of Personal Information

5.1.1 The University will only collect personal information that is expressly authorized by an enactment of Alberta or Canada, for the purposes of law enforcement or that relates directly to and is necessary for an operating program or activity of the University. Personal information will be

collected directly from the individual who is the subject of the information except as otherwise permitted by legislation.

- 5.1.2 Authorized persons may collect only minimum amount of personal information for or on behalf of the University. Authorized persons will provide a personal information collection notice to individuals from whom personal information is collected.
- 5.1.3 Personal information will be collected directly from the individual who is the subject of the personal information. Indirect collection of personal information is only permitted under those circumstances set out in the FOIP Act.
- 5.1.4 Where the University receives unsolicited personal information from an individual, the unsolicited personal information may, in the University's discretion, be retained for 12 months after which it may be destroyed if the provider of the information has not accessed any University services within that period.

5.2 **Management of Personal Information**

- 5.2.1 Authorized persons may only access personal information that is in the custody of the University when there is a legitimate need to use such information, and only to the level of detail necessary to enable them to properly perform an operating activity or program of the University.
- 5.2.2 The use of personal information must be in accordance with the purpose for which the information was collected or for a use consistent with that purpose except in circumstances where the individual who is the subject of the personal information has consented to the use of the information for a different purpose.
- 5.2.3 Access to and use of personal information that is in the custody or under the control of the University by external organizations or individuals who are not members of the University community, with whom the University has entered into an information sharing or collecting undertaking, will be governed by an information sharing agreement which will contain standard information security safeguards and confidentiality provisions.
- 5.2.4 Personal information collected by the University may be retained for no less than one year, after which the personal information may be destroyed according to the retention periods contained in the University's Records Retention and Disposition Schedule.

- 5.2.5 Personal information that is in the custody or under the control of the University will only be disclosed in accordance with the FOIP Act.
- 5.2.6 Where practicable and before an authorized routine disclosure, the University may anonymize or transform an individual's personal information into non-identifying personal information if the end-user of the information does not require or should not obtain the identity of the subject of the personal information.
- 5.2.7 An individual who believes there is an error or omission in his or her personal information that is in the custody or under the control of the University may submit a written request for correction to the University.
- 5.2.8 The retention and disposition of records will be in accordance with the University's Records Retention and Disposition Schedule and the Records Destruction Procedure.

5.3 Employees' Personnel Files

- 5.3.1 Employees who wish to access or request the correction of their employment records with the University will follow the procedure in the Access to Records and Correction of Personal Information Procedure.
- 5.3.2 Except when their employment-related duties and responsibilities require, employees of the University may not access, without authorization by their managers, anyone's employment records, including their own record that is in the custody or under the control of the University.

5.4 Confidentiality of Video Surveillance

- 5.4.1 Video surveillance on University premises may only be conducted by Security Services. Personal information collection notices will be installed at building entrances that are closest to surveillance camera locations.
- 5.4.2 The use or disclosure of images captured by audiovisual recording on surveillance cameras on University premises is governed by this policy and associated procedures.
- 5.4.3 Any covert video surveillance must receive prior approval from the privacy department.

5.5 Access Controls

5.5.1 The University will protect personal information from unauthorized access, use, disclosure or destruction through a system of administrative, physical and technical controls, which includes but is not limited to:

- (i) restricting access to personal information that is stored in an electronic format to authorized persons by requiring login credentials;
- (ii) storing personal information in locations which are not generally accessible to members of the University community or the general public; and
- (iii) securing the rooms and filing cabinets that contain personal information during those times that an authorized person is not present.

5.6 Exclusion from Application

5.6.1 Research information and teaching materials that are in the custody or under the control of the University are not accessible to the general public through an access request submitted under the FOIP Act.

5.7 Non-compliance

5.7.1 Employees of the University may not collect, use, disclose or destroy records in contravention of the FOIP Act or this policy.

5.7.2 Instances of possible non-compliance with the FOIP Act and this policy must be immediately reported to the privacy department which will conduct an investigation into the matter.

5.7.3 Non-compliance with this policy may result in disciplinary action up to and including the termination of contract or appointment.

FACT SHEET

Relevant Dates

Approved: 2015.02.26
Effective: 2015.02.26
Next Review: 2020.02

Source

Modification History:

2015.02.26 Approved by Board Motion 02-02-26-2014/15. This is a new policy that documents provisions relating to the collection, use and disclosure of personal information by employees of MacEwan University.

2018.11.19 Minor revision to add an associated document. Approved by Policy Sponsor on November 19, 2018.

2021.11.01 Minor revision to update position title. Approved by Policy Sponsor.

Authorization

Office of Accountability: General Counsel

Office of Administrative Responsibility: Privacy and Information Management Department

Approved by: Board of Governors

Contact Area: Privacy and Information Management Department

Authority: Alberta's *Freedom of Information and Protection of Privacy Act*

Related and Associated Matters

Associated Procedures:

D7500-1: Access to Records and Correction of Personal Information
D7500-2: Use of Personal Information for Research Purposes
D7500-3: Legal Hold
D7500-4: Records Destruction
Privacy and Security Assessment Intake Questionnaire

Related Policies:

D7510: Records Management
C5052: Ethical Review of Research
D7990: Legal Resources
D7225: Electronic Mail
D7230: Information Security
E1050: Student Records