INFORMATION ACCESS, PRIVACY AND SECURITY POLICY

Policy Type:	Institutional	**Initially Approved:**	March 6, 2026
Policy Sponsor:	President and CEO	**Last Revised:**	March 6, 2026
Primary Contact:	University Secretariat Office	**Review Scheduled:**	March 2029
Approver:	President and CEO		

A. INTENT

This policy is aligned with the new Alberta *Access to Information Act* ("ATIA") and Alberta *Protection of Privacy Act* ("POPA"), which came into effect in June 2025.

The ATIA ensures individual right of access to information and the POPA protects the personal information of the public, and employees of public bodies operating in Alberta. Alberta University of the Arts (AUArts) is bound by the requirements of ATIA and POPA, and collects, uses, and discloses personal information in accordance with the provisions outlined in the Acts. This policy establishes the principles and processes for managing AUArts information in compliance with ATIA and POPA.

B. SCOPE

This policy applies to:

1. All authorized users of the University's information, including board of governors, employees, third party contractors, students, and volunteers providing services on behalf of AUArts;
2. All recorded information, in whatever form or medium (paper, digital, audio-visual, graphic) created or received while carrying out AUArts' mandated functions and activities; and
3. All facilities and equipment required to collect, manipulate, transport, transmit, or keep AUArts information.

C. ROLES AND RESPONSIBILITIES

1. The President and CEO of AUArts is appointed as the designated head of AUArts and is responsible for the University's obligations under the Acts.
2. In accordance with the Acts the President and CEO can and has delegated the administrative duties required under ATIA and POPA to the University Secretary who serves as the Access to Information and Privacy Officer. The University Secretary provides guidance and advice when individuals have access and privacy related questions.

3. In collaboration with the President and CEO's Cabinet the University Secretary is responsible for:
    a) promoting, monitoring, and reporting on compliance with ATIA and POPA and with university privacy, records management policies, including:
        i. Providing advice on and responding to Access to Information Requests;
        ii. Providing access and privacy training;
        iii. Providing ongoing assessment of privacy risks; and
        iv. Investigating concerns about alleged privacy breaches and violations.
4. Managers are responsible for:
    a) making reasonable efforts to ensure that the management of Personal or Confidential Information in the custody or under the control of their units meets the requirements of ATIA, POPA, this policy and its associated procedures;
    b) reporting any alleged privacy Breaches or Violations in accordance with the AUArts' Privacy Breach Response Procedure; and
    c) Conducting risk-based Privacy Impact Assessments.
5. All employees who collect, access, use, disclose, maintain and dispose of Personal Information are in a position of trust. employees are responsible for:
    a) treating all Personal Information to which they receive access in accordance with POPA and this policy;
    b) responding to
    c) consulting as necessary with the appropriate authority regarding the requirements in POPA, this policy, and its associated procedures; and
    d) reporting any alleged privacy Breaches or Violations in accordance with the AUArts' Privacy Breach Response Procedure.
6. The university requires third party contractors whose work on behalf of the university involves the collection, use or disclosure of Personal Information to comply with ATIA, POPA, this policy and its associated procedures.

D. POLICY STATEMENT

1. PRINCIPLES

The university collects Personal Information from students, employees and others in order to fulfill its mandate under the *Post-Secondary Learning Act*. AUArts is committed to providing full informational accountability and to protecting the privacy of individual citizens and its employees.

1.1 **Accountability.** AUArts is responsible for protecting the confidentiality of personal information in its custody or under its control in compliance with the applicable privacy legislation.

1.2 **Openness.** AUArts develops and follows access, privacy and security policies and practices that are compliant with legislation. Such policies and practices are available upon request.

1.3 **Collection of Personal Information**. AUArts collects personal information only for authorized purposes and collects the least amount of personal information with the highest degree of anonymity required for the authorized purpose. In compliance with POPA when collecting personal information directly from an individual, the individual is informed of the purpose for which the information is collected, the legal authority for the collection, and the title, business address and telephone number of the person who can answer questions about the collection.

1.4 **Limited Use and Disclosure of Personal Information.** Personal information is only used and disclosed in accordance with the purpose for which it was collected, unless alternate use or disclosure is authorized or required by law, or with the knowledge and consent of the individual.

1.5 **Accuracy.** AUArts makes all reasonable efforts to ensure that both general information and personal information created or received by AUArts is accurate and complete. Individuals who believe there is an error or omission in their personal information have a right to request correction or amendment of the information as set out in POPA.

1.6 **Right of Access.** Individuals have a right of access to all information that is in AUArts custody or control, subject to limited and specific exceptions as set out in the Acts.

1.7 **Safeguards.** AUArts protects personal information in its custody or control by deploying reasonable security measures and practices to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or destruction.

1.8 **Compliance Challenges.** Individuals are encouraged to bring any concerns or issues regarding access and privacy at AUArts to the University Secretary for discussion and response. Individuals may appeal to the Information and Privacy Commissioner of Alberta to review or investigate AUArts right of access or correction responses, or any policies or practices that they feel are not in compliance with legislative requirements.

2. COLLECTION OF PERSONAL INFORMATION

2.1 AUArts collects personal information only if:

a) The collection is expressly authorized by an enactment of Alberta or Canada;
b) The information is collected for the purposes of law enforcement;
c) The information relates directly to and is necessary for an operating program or activity of the public body.

2.2 AUArts collects personal information directly from the individual, or their authorized representative, unless indirect collection is authorized under Sections 5 or 13 of POPA in the following circumstances:

a) indirect collection of the information is authorized by the individual, another Act or regulation, or the Alberta Information and Privacy Commissioner;
b) the information may be disclosed to the public body under the disclosure provisions;
c) the information is collected in a health and safety emergency and the individual is unable to provide the information, or direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or of any other person;
d) the information is about a designated emergency contact;
e) the information is collected for determining suitability for an honour or award, or to determine or verify eligibility for participation in a program or to receive a benefit, product, or service from the public body;

3. DATA MATCHING

3.1 As permitted under POPA Section 17 AUArts may carry out Data Matching to create data derived from personal information for the following purposes:
   a) Research and analysis
   b) Planning, administering, delivering, managing, monitoring or evaluating a program or service

3.2 For the purpose of Data Matching AUArts must not collect personal information directly from the individual, but can:
   a) Get the personal information from another public body
   b) Use personal information already in its custody or control

3.3 All data matching activities between two public bodies must undergo a Privacy Impact Assessment and security review, including assessment of re-identification risk and bias.

4. CREATION OF NON-PERSONAL DATA

4.1 The University may create Non-personal Data from the information it collects for the following purposes:
   a) Research and analysis
   b) planning, administering, delivering, managing, monitoring or evaluating a program or services

4.2 The University will ensure:
   a) To the extent possible, that the identity of an individual who is the subject of non-personal data cannot be re-identified from the data. Prior to creating non-personal data, the risk of re-identification will be assessed and security measures to reduce the risk will be documented.
   b) That the methods to create the non-personal data identify and account for potential bias in the non-personal data
   c) That a record is created which identifies, the IT security classification of the non-personal data.
   d) The accuracy of the data if the non-personal data will be used to inform decisions about programs of services at AUArts.

5. PROTECTION AND RETENTION OF PERSONAL INFORMATION AND NON-PERSONAL DATA

5.1 The University must protect Personal Information, Sensitive or Confidential Information, Research Records and Non-personal Data by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, modification, or destruction. These include but are not limited to the following:
   a) Physical safeguards: securing records in locked rooms or cabinets, limiting access to areas that hold personal information, restricting access to server rooms and network infrastructure;
   b) Administrative safeguards: policies and related training, confidentiality agreements, identity authentication procedures;
   c) Technical safeguards: using password protection, multi-factor authentication and data encryption, access control systems, locking computers when left unattended, limiting third party vendor access as recommended by referenced Information Technology procedures;

d) Portable device security: enabling password access, keeping mobile device physically secure (e.g. locking cable for laptop).

5.2 AUArts conducts Privacy Impact Assessment for all new systems, projects, programs or activities and substantially modified systems or activities in accordance with POPA. The nature and extent of the assessment will be in accordance with guidance provided by the Office of the Information and Privacy Commissioner of Alberta.

5.3 Official records will be disposed of securely and regularly as per the University's Records Management Procedure and Retention Schedule, consistent with the Act.

5.4 In accordance with POPA Section 18 (1) once AUArts has finished using data derived from Data Matching Personal Information, for the purpose for which it was created, the public body must destroy the data derived from personal information or transform it into non-personal data.

6. ACCESS TO INFORMATION

6.1 Upon the University receiving a written access to information request, in writing, employees shall immediately forward the request to access.privacy@auarts.ca.

6.2 According to Section 6 of ATIA, individuals may at any time make a written request to the University to access any record in the custody or under the control of AUArts, including a record including their own Personal Information held by the University.

6.3 The University will grant access, subject to the specific and limited exceptions to disclosure as outlined in Division 2 of ATIA, to any individual who requests access to any record containing general information or the applicant's Personal Information in the University's control.

6.4 The University may disregard a request in accordance with Section 9(1) of ATIA.

6.5 Employees will be notified if it appears they have records responsive to an Access to Information request and will be asked to do a thorough and timely search.

6.6 Employees must not dispose of or alter any records relating to an access to information request, even if the records are scheduled for destruction under the Records Management Retention Schedule.

7. ACCURACY AND CORRECTIONS OF PERSONAL INFORMATION

7.1 Personal Information collected, used and disclosed by the University shall be as accurate, complete and up to date as is necessary for the purposes for which it is to be used.

7.2 In accordance with Section 7.1 of POPA individuals have the right to request corrections of errors or omissions to their own Personal Information. Individuals may make a request a correction directly to the unit responsible who collected their personal information or to access.privacy@auarts.ca who can facilitate the request.

8. TRAINING AND AWARENESS

8.1 All employees, third party service providers, members of the board of governors and volunteers who collect, access, use, or manage AUArts records and Personal Information must complete privacy and access to information training as part of onboarding and on a recurring three-year basis.

8.2 Refresher training, updates on legislative changes, and topic-specific awareness (e.g. privacy impact assessments, breach prevention, new policies) will be provided to relevant individuals as needed.

E. DEFINITIONS

Authorized representative: Any person who can exercise the rights or powers of an individual. This includes the right of access to an individual's personal information and the power to provide consent for disclosure of such information. This may include:

- An executor or administrator of the estate of an individual who is deceased, for purposes of administering the estate;
- A guardian or trustee of a dependent adult, according to appointment under law:
- An agent under a personal directive, in accordance with the directive:
- An individual who is acting under specific provisions of a power of attorney:
- A guardian of a minor under 18 years of age, if the exercise of the rights or powers of the guardian would not be an unreasonable invasion of the personal privacy of the minor; or
- An individual acting with the written authorization of an individual.

Access to Information Request: A formal request for access to information made under the Access to Information Act (ATIA), Alberta, including both General and Personal access to information requests.

Collection: To gather, acquire or obtain personal information about an individual, from any source, including third parties.

Collection documents: Any University form, electronic or physical, that requests and collects personal information from a person.

Consent: Agreement by an individual to the disclosure of their own personal information to a third party. The consent must include:

- An authorization for AUArts to disclose the information specified in the consent;
- The purpose for which the information may be disclosed;
- The identity of the person to whom the information may be disclosed;
- An acknowledgement that the individual providing the consent has been made aware of the reasons why the

information is needed and the risks and benefits to the individual of consenting or refusing to consent;
- The date the consent is effective and the date, if any, on which the consent expires; and
- A statement that the consent may be revoked at any time by the individual providing it.
- A consent or revocation of consent can be provided in writing or electronically. Electronic consent is valid only if the level of authentication is sufficient to identify the individual who is granting the consent or revoking the consent.

Custody and Control: Custody is the effective physical possession of information; control is responsibility and accountability for making decisions about the handling of information, regardless of whether AUArts has custody of the information. AUArts has control over any information it has created or received as part of its mandated functions and activities, regardless of the location of the information or the time of collection, use, or disclosure.

Data Matching: Linking personal information between 2 or more databases or other electronic sources of information to create new data. Includes the merging of two or more sources to create new information about an individual. The personal information in the data must still be identifiable.

Disclosure: Giving access to or making the information in AUArts' custody or control available to a person or organization external to AUArts.

Electronic Record: A record that exists at the time a request for access is made or that is routinely generated by a public body that can be any combination of texts, graphics, data, audio, pictorial or other information represented in a digital form that is created, maintained, archived, retrieved or distributed by a computer system.

Individual: Any person, living or deceased, regardless of residency, citizenship, or status. In addition, the authorized representative of the individual.

Non-Personal Data: Data, including data derived from personal information, that has been generated, modified or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the POPA regulations.

Notification: An explanation of policies, procedures, consequences, and risks related to the collection, use or disclosure of an individual's personal or personal employee information. AUArts must properly inform and notify individuals and

employees that personal information is being collected, the purposes for which it is being collected, and who may be contacted at AUArts if an individual has questions about the management of their personal information.

Personal Employee Information: Personal information collected, used, or disclosed solely for the purposes of establishing, managing, or terminating an employment or volunteer relationship.

Personal Information Bank (PIB): An information repository that is organized or retrievable by an individual's name or other identifier, such as a student or employee id.

Personal Information: Recorded information about an identifiable individual, including the following examples listed in Section 1(r) of ATIA:

- name
- race
- colour
- religion
- age
- sex
- marital status
- family status
- home or business address or telephone numbers
- national or ethnic origin
- political beliefs or associations
- identifying numbers
- fingerprints or blood type
- educational, financial, employment, criminal records
- opinions about the individual
- individual's personal views or opinions (except opinions about others)

Personal information under Section 20 (2) of ATIA that is not normally exempted from disclosure:

- business title, address, or telephone number of an individual
- opinions contained in work product
- classification, salary range, discretionary benefits, or employment responsibilities of public body employees
- financial and other details of a contract to supply goods or services to a public body
- information about a license, permit, financial or other discretionary benefit granted to an individual by a public body
- the information is about an individual who has been dead for 25 years or more
- the information is about an individual's enrolment at a school, attendance at a public event, or receipt of an award granted by a public body.

Privacy Breach: An unauthorized disclosure, use, destruction, loss, removal, modification, or interruption in the availability of personal or health information.

Privacy Impact Assessment (PIA):	A review and explanation of proposed changes in administrative practices or information systems affecting the collection, use, disclosure, or security of personal information under the custody and control of a public body.
Privacy Violation:	A security gap or procedural failure where personal information protection may have been compromised, but no confirmed Breach has occurred.
Record:	Any electronic record or other record in any form in which information is contained or stored, including information in any written, graphic, electronic, digital, photographic, audio or other medium. This does not include software or any mechanism that produces records.
Research:	Academic, applied, or scientific research that necessitates the use of individually identifying personal information. Public bodies may only provide personal information for research purposes under strict conditions, in a written agreement.
Research Records:	Research information assets supporting both research and operational needs. This includes administrative information and records produced for analytic or evidentiary purposes. Research records include those documents and records and materials captured by or for a researcher that are necessary to document, reconstruct, evaluate, and validate research results and the events and processes leading to the acquisition of those results. Research records may be in many forms including but not limited to notebooks, survey documents, questionnaires, interview notes, transcripts, machine generated data or performance outputs, recruitment materials, consent forms, correspondence, other documents, computer files, audio or video recordings, photographs including negatives, slides, x-ray films. With regard to research involving human participants or animal use, research records usually relate to the data collected about the subjects of the research.
Routine Request for Personal Information:	Requests to access personal information about themselves so long as the information requested does not contain third-party personal information, does not require, or allow the public body to withhold information according to the specific and limited exceptions under ATIA and/or POPA.
Sensitive or Confidential Information:	Sensitive or confidential information refers to all information that has been collected or compiled in the conduct of operating the programs and services of the University and may include, but is not limited to:

- Confidential business information of third parties;
- Confidential information collected or compiled in the process of hiring or evaluating employees of the University;
- Information collected or compiled in the process of law enforcement investigations;
- Advice, proposals or recommendations, consultations or deliberations of the governing and administrative authorities of the University;
- Information, the disclosure of which would harm the economic interests of the University;
- Any information to which legal privilege including client-solicitor privilege may apply

Severing: In an access to information request, separating or hiding/redacting information in a document that should or cannot be released so that the remainder of the document can be disclosed.

Use: Use of information by AUArts employees for an authorized purpose that is authorized by policy or law.

F. RELATED POLICIES

- Board of Governors: Code of Conduct Policy
- AUArts Records Management Policy and Retention Schedules

G. RELATED LEGISLATION

- Access to Information Act, Alberta
- Post-Secondary Learning Act, Alberta
- Protection of Privacy Act, Alberta

H. RELATED DOCUMENTS

- Privacy Impact Assessment Guide

I. REVISION HISTORY

Date (mm/dd/yyyy)	Description of Change	Sections	Person who Entered Revision (Position Title)	Person who Authorized Revision (Position Title)
03/06/2026	New policy. Addresses new access and privacy legislation.	All	University Secretary	President and CEO