Procedure

ACCESS TO INFORMATION PROCEDURE

Procedure Section:	Privacy Management Program	**Effective Date:**	June 11, 2026
Policy Owner:	Vice President, Administration & CFO	**Last Revised:**	June 4, 2026
Policy Administrator:	Information Access & Legislative Compliance	**Review Scheduled:**	Every 4 years
Approver:	Executive Leadership Team		
The official controlled version of this document is held with the Legislative Compliance / Policy & Procedure Coordinator.			

A. PROCEDURES

1. Overview

Keyano College is committed to ensuring that is it an open, accessible and accountable public body. Under the Alberta Access to Information Act (ATIA) we aim to balance the public's right to know information while protecting confidential information subject to the Alberta Protection of Privacy Act (POPA).

This procedure establishes roles and responsibilities for the access to records both internal and by the public. Keyano College has a duty to assist applicants under ATIA.

2. Responsibilities

a. The President and CEO as Head of the Public Body is responsible to:

i. Delegate duties to designated Access and Privacy Officer
ii. Uphold the Access to Information Act

b. Executive and Senior Leadership:

i. Uphold the Access to Information Act
ii. Ensure that all reporting staff take the mandatory access to information training
iii. Respond to requests for information from the Records Management and Information Access & Legislative Compliance in a timely manner to allow the College to meet legislated timelines.
iv. Instruct all reporting staff to adhere to information requests as above.
v. Adhere to all records holds as directed by the Records Management and Information Access & Legislative Compliance.

c. Records Management and Information Access & Legislative Compliance:

i. Create procedures and processes to ensure compliance with the ATIA.
ii. Coordinate responses to access to information requests including:
    1. Notification to departments of search and retrieval of records requirements

2. Respond to applicants fairly and without prejudice
3. Collect and prepare records for release
4. Prepare list of records approved for proactive release

iii. Liaison with the Office of the Information and Privacy Commissioner:

1. In responding to access to information reviews
2. Reporting of annual statistics
3. Responding to investigations or orders of the Commissioner

iv. Reports to the President and CEO as Head of the Public Body

d. Information Technology:

i. Ensure that all systems meet or exceed privacy protection legislation requirements
ii. Create procedures and processes to ensure all data systems comply with the POPA
iii. Make reasonable security measures for the protection of data and unauthorized access, use or disclosure of data.

e. Employees:

i. Employees only have access to personal information that is needed and necessary to do their jobs.
ii. Attend mandatory access to information training
iii. Take reasonable security measures to protect against unauthorized use and disclosure of personal information.
iv. Report information breaches or cybersecurity issues as soon as they are aware of them in accordance with the Data Breach of Security Policy and Procedure, and the Privacy Breach Procedure
v. Reply in a timely manner to requests for records by the Records Management and Information Access & Legislative Compliance
vi. Adhere to all records holds as directed by the Records Management and Information Access & Legislative Compliance
vii. Follow the process for the creation, documentation, use and disclosure of non-personal data, data matching, synthetic data and data derived from personal information.

3. Access to Personal Information

a. Employee Access – employees will only have access to personal information that is needed and necessary to perform their duties.
   i. Employees are responsible to apply Security Classifications to records they create or are responsible to manage in accordance with the Security Classifications Guidelines or seek guidance from the Records Management role and Information Access & Legislative Compliance regarding the classification of newly created records.
   ii. Role based security structures will applied to all systems and controlled by Information Technology.
   iii. Access to systems must be approved by employee supervisor and justified by the employee's role and responsibilities.
   iv. Failure to comply with the procedure constitutes a misconduct and may be handled under the College's Code of Conduct.

b. Routine Disclosure – records classified as Public under the Security Classification Guidelines is accessible and intended for everyone.
    i. This includes non-personal, general, published information and those records required to be made public as per the Post-Secondary Learning Act, or other legislation.
    ii. Some material may be available on the Keyano public facing internet page or may be requested from the responsible department without a formal ATIA request.
    iii. Keyano may set fees for some copies of recorded information or record that is available without an ATIA request as per policy or procedures.

c. ATIA Request
    i. An ATIA request may be filed to access information that is not available through routine disclosure.
    ii. An ATIA request must be filed in writing to the Information Access & Legislative Compliance.
        1. Must be accompanied by the fee of $25 for a request of general information (non-continuing request), or $50 for general information (continuing request).
        2. **There is no fee to request personal information about yourself**
        3. The request must provide enough detail to enable the College to locate and identify responsive records.
            a. The Information Access & Legislative Compliance will contact the applicant if clarity regarding the request is needed.
    iii. The College has **30 business days** to reply to a request however time may be extended if
        1. The applicant agrees
        2. A large number of records are requested, and more time is needed to process the request or
        3. More time is needed to consult with a third party subject to ATIA section 36
    iv. In compliance with section 9 of ATIA a request may be disregarded by the College if:
        1. Responding to the request would unreasonably interfere with the College's operations or amount to an abuse of the right to make a request because the request has been made repeatedly or in a systematic nature
        2. The request is abusive, threatening, frivolous or vexatious or made in an abusive or threatening manner.
        3. The information has already been provided to the applicant or has been made available to the public.
        4. There is insufficient information to enable the College to locate and identify the record within reasonable time with reasonable effort.
        5. The request is overly broad or incomprehensible.
    v. The Collage may declare a request abandoned if
        1. The applicant does not reply to the request for further information that is necessary to process the request.
        2. The applicant fails to pay the initial processing fees or additional fees as required under ATIA.
    vi. A request to the College may be transferred to another public body within 15 days of receiving a request if it is determined that
        1. The record was produced by or for the other public body
        2. The other public body was the first to obtain the record
        3. The record is the custody or control of the other public body.

vii. The Information Access & Legislative Compliance will coordinate the response to all ATIA requests.

d. Exceptions to Disclosure
   i. All exceptions to disclosure will be applied by the Information Access & Legislative Compliance in accordance with ATIA.

e. Right to ask for a review
   i. An applicant who disagrees with a decision regarding their request can request the Office of the Information and Privacy Commission of Alberta (OIPC) to review any decision, act or failure to act of the College.
      - Requests must be made in writing to the OIPC and Keyano within 60 business days of receiving notification of a decision by the College.

B. DEFINITIONS

(1)	**ATIA:**	means the Alberta Access to Information Act.
(2)	**Control:**	means the College has authority to manage, restrict, or administer the collection, use and disclosure of a record.
(3)	**Custody:**	means the College has physical possession of the record.
(4)	**Data Derived from Personal Information:**	means data (i) created by data matching, and (ii) that identifies any individual whose personal information was used in the data matching.
(5)	**Data Matching:**	means linking personal information between 2 or more databases or electronic sources of information.
(6)	**Employee:**	means a person who performs a service for the College as an appointee, volunteer or student or under a contract or agency relationship with the College.
(7)	**Non-Personal Data:**	means data, including data derived from personal information, that has ben 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 under POPA Ministerial Regulations.
(8)	**OIPC:**	means the Office of the Information and Privacy Commissioner of Alberta.
(9)	**Personal Information:**	means recorded information about an identifiable individual including, but not limited to name and contact information, age and gender; unique identification numbers (i.e. SIN, driver's license, student number); gender, race, ethnic origin, citizenship; income or marital status; family or marital status; education,

		employment, health or biometric information; and criminal history.
(10)	**POPA:**	means the Alberta Protection of Privacy Act.

C. RELATED LEGISLATION

- *Alberta Access to Information Act (ATIA)*
- *Alberta Protection of Privacy Act (POPA)*
- *Government of Alberta Public Disclosure of Travel and Expenses Policy*
- *Post Secondary Learning Act*
- *Public Sector Compensation Transparency Act*

D. RELATED DOCUMENTS

- ATIA Request Form
- Code of Conduct Policy
- Data Breach of Security Policy and Procedure
- Data Quality Assurance Process
- Employee Progressive Discipline Policy and Procedure
- Privacy Breach Procedure
- Privacy Policy & Procedure
- Public Disclosure of Information on Travel
- Records Classification and Retention Schedule
- Safe Disclosure Policy and Procedure
- Security Classifications Guidelines

E. REVISION HISTORY

Date (mm/dd/yyyy)	Description of Change	Sections	Person who Entered Revision (Position Title)	Person who Authorized Revision (Position Title)
6/4/2026	New Procedure.		Records Management & Information Access Advisor	Vice President, Administration & CFO