Keyano College

# Procedure

## PRIVACY 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 the protection of personal information in accordance with the Alberta Protection of Privacy Act (POPA). In doing so, the College implements reasonable security arrangements to protect the information in our custody and control against unauthorized collection, use, access, disclosure, or destruction.

This procedure establishes roles and responsibilities for protection of privacy in the collection, use, disclosure and disposition of personal information.

### 2. Responsibilities

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

i. Delegate duties to designated Access and Privacy Officer
ii. Uphold the Protection of Privacy Act
iii. Authorize the investigation of privacy issues or breaches in the event they become aware of an issue.
iv. Signing authority for Privacy Impact Assessments
v. Signing authority for disclosure of non-personal data under the Data Quality Assurance Process for the Creation of Non-Personal Data

b. Executive and Senior Leadership:

i. Uphold the Protection of Privacy Act
ii. Ensure that all reporting staff take the mandatory access and privacy training
iii. Report any privacy issues or breaches if they become aware of an issue
iv. Ensure that Records Management and Information Access Advisor is consulted regarding projects or programs that may require a Privacy Impact Assessment (PIA)

v. Ensure that the correct staff members are assigned to provide information for the completion of PIAs.

c. Records Management Role and Information Access & Legislative Compliance:

i. Information Access & Legislative Compliance role is the designated Privacy Officer as per the delegation letter issued by the President
ii. Create procedures and processes to ensure the protection of privacy
iii. Advise the College on the protection of privacy including
- Collection, use and disclosure of personal information
- Reasonable security measures
- Security structures for information systems in conjunction with Information Technology, including user-based security access
- Coordinate with Information Technology department in the event of cybersecurity incident
- Review and draft Collection Notices to adhere to Protection of Privacy Act

iv. Conduct privacy investigations as directed by the President.
v. Conduct and coordinate the completion of Privacy Impact Assessments (PIAs) as required, maintain a registry of all completed PIAs, file PIA's with OIPC as required.
vi. Respond to requests for the correction of personal information and coordinate the documentation, response, notification of other third party if required, and direction to the responsible department to correct or annotate the record.
vii. Conduct assessments of non-personal data prior to the release
viii. Liaison with the Office of the Information and Privacy Commissioner
- In responding to privacy breach complaints
- Reporting cybersecurity or privacy breaches as required under the Protection of Privacy Act
- Filing of privacy impact assessments
- Reporting of annual statistics
- Responding to investigations or orders by the Commissioner

ix. Create and maintain Privacy Management Program
x. Maintain Personal Information Banks (PIB) Directory
xi. Develop and deliver privacy training to staff.
xii. Maintain statistics, reports, KPIs, etc. on the Privacy Management Program

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 Protection of Privacy Act
iii. Participate in PIAs as required
iv. Make Records Management and Information Access Advisor aware of any project that requires PIAs
v. Make reasonable security measures for the protection of data
vi. Coordinate with the Access and Privacy Officer in the event of cybersecurity incident particularly with regards to the investigation, documentation, reporting and remediation.

e. Departments and Employees:

i. Employees only have access to personal information that is needed and necessary for them to do their job

ii. Attend mandatory privacy training
iii. Take reasonable security measures to protect against the unauthorized collection, use or disclosure of personal information
iv. Only collect and use personal information for the purpose stated in the Collection Notice
v. Report information breaches or cybersecurity issues as soon as they are aware of them in accordance with the Data Breach of Security Policy or Procedure, and the Privacy Breach Procedure
vi. Follow the Data Quality Assurance Process for the creation, documentation, use and disclosure of Non-Personal data, Data Matching, Synthetic Data, and Data Derived from Personal Information
vii. Inform the Records Management and Information Access & Legislative Compliance regarding requests for correction of personal information and follow the direction of the Records Management and Information Access & Legislative Compliance regarding corrections or annotations.

**3. Protection of Personal Information**

a. The College will take reasonable security measures to safeguard and protect the information in its Custody and Control against the risk of unauthorized access, collection, use disclosure or destruction. Including:

i. Following all applicable policies, procedures and legislation.
ii. Ensure the protection of highly sensitive information and the routine disclosure of publicly available records by assigning security classifications to records as per the Keyano Security Classifications Guidelines
iii. Set user-based security access for all information systems and ensure audit logs are appropriate structured and monitored.
iv. Periodically Keyano College will evaluate their privacy protocols to identify and evaluate issues, escalation, containment and compliance. This may be in conjunction with Information Technology tabletop cybersecurity exercises.
v. Monitor automated systems security controls with audits, security threat and risk assessments, including vulnerability assessments and penetration testing, algorithmic impact assessments.

b. The College will conduct Privacy Impact Assessments (PIAs) in accordance with POPA Ministerial Regulation, for any new, or a substantial change to an existing, administrative practice, program, project or service that will involve the collection, use or disclosure of personal information.

i. The College must submit PIAs to the OIPC under the circumstances outlined in the POPA Ministerial Regulation.
ii. Information Access & Legislative Compliance will coordinate the completion of PIAs in conjunction with Information Technology and the responsible department.

c. Keyano will maintain and publish a directory of Personal Information Banks (PIB's). The directory will document the:

i. Location of storage
ii. Categories of personal information it holds
iii. Categories of individuals (such as students, minors, adults, staff)
iv. Specific purpose for data collected, used, and disclosed
v. Sensitivity of the information

vi. Security classification

d. The creation, use and disclosure of non-personal data must follow the Data Quality Assurance Process for the Creation of Non-Personal Data.

e. Any staff who becomes aware of a data or privacy breach must report immediately as per the Data Breach of Security Policy and the Privacy Breach Procedure.

## 4. Collection of Information

a. Personal information can only be collected when is needed for the purpose of an approved activity by the College, or to meet requirements of legislation.
   i. Where practical, the College will collect personal information directly from individuals.
   ii. At the time of collection, a Collection Notice must be provided to the individual. This notice must include:
      - The legal authority to collect personal information.
      - The purpose of the collection and how the information will be used.
      - The intend, if any, at the time to input the information into an automated system to generate content to make decisions, recommendations, or predictions.
      - The title and contact information for the employee or department to whom questions about the collection and use of the personal information can be directed.
   iii. Collection Notices must be applied to all forms of personal information collection and can be supplied in writing, verbally, and/or displayed.
   iv. Only the personal information required to complete the business activity can be collected.
   v. Activities or business functions that require the collection of personal information should seek the review of the Information Access & Legislative Compliance to ensure compliance with the collection of personal information.

b. Reasonable steps must be taken to ensure the accuracy of all personal information and such information must be retained in compliance with POPA.
   i. Personal information collected that will be used to make a decision about an individual must be maintained for a minimum of one year, unless the College and the individual agree to a shorter period.
   ii. Individuals have the right to request the correction of their personal information; however, we can not correct an opinion including a professional or expert opinion. In those cases, an annotation may be made to the record to document the requested correction.
   iii. Requests to have personal information corrected must be directed to the Information Access & Legislative Compliance to ensure appropriate review and documentation.
      1. The Information Access & Legislative Compliance will:
         a. Review the request for correction
         b. Provide direction to the department responsible for the personal information.
         c. Notify other public bodies if required under POPA
         d. Respond within 30 days to the applicant to provide notice of correction or annotation as required under POPA.

**5. Use of Personal Information**

a. Personal information can only be used for the purpose for which it is collected or for a consistent purpose, or in accordance with a legislation of Alberta or Canada.
b. Employees may only access and use personal information as is needed to fulfil their employment obligations.
c. Written Informed Consent must be obtained from an individual to use personal information for a purpose other then the purpose stated at the time of collection.
d. If Keyano creates Non-Personal Data from Personal Data or Data Matching Employees are required to follow the Data Quality Assurance Process to document
    i. The Personal Information used to create the data
    ii. The purpose for creating the data
    iii. The method for creating the data
    iv. Verification that de-identification methods are effective and cannot be easily reversed (re-identified).

**6. Disclosure of Personal Information**

a. Disclosure of Personal Information will be conducted in accordance with the Access to Information Procedure.
b. Disclosure of Non-Personal Data to a third party must be done in accordance with the Data Quality Assurance Process.
    i. If the disclosure is to a third-party approval of the President is required to be documented as per the Data Quality Assurance Process.

**7. Destruction of Personal Information**

a. Business records that contain Personal Information will be retained as per the Keyano Records Classification and Retention Schedule and will be disposed in accordance with the Records Disposition Procedure.
b. Transitory documents that contain personal information must be placed in a confidential shredding bin for secure destruction.

**8. Compliance**

a. Failure to comply with this procedure could be a breach of the College's Code of Conduct and may result in actions under the Employee Progressive Discipline Policy and Procedure.

**9. Complaints**

a. An individual can make a complaint regarding the collection, use or disclosure of their personal information to College

    i. Keyano will respond with in 30 days to the complaint.

b. Once receiving Keyano's response to the complaint, an applicant may ask the Office of the Information and Privacy Commission of Alberta (OIPC) to review any decision, act or failure to act of the College.

    i. Requests must be made in writing to the OIPC 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)** | **Business records:** | means records that document business activities, functions, and decisions that staff have a duty to document. |
| **(3)** | **Control:** | means the College has authority to manage, restrict, or administer the collection, use and disclosure of a record. |
| **(4)** | **Custody:** | means the College has physical possession of a record. |
| **(5)** | **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. |
| **(6)** | **Data Matching:** | means linking personal information between 2 or more databases or electronic sources of information. |
| **(7)** | **Duty to Document:** | means that employees must document the actions and decisions they make in the course of their duties. |
| **(8)** | **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. |
| **(9)** | **Highly Sensitive Information/Data:** | means biometric information about an individual, financial information about an individual, personal information respecting a minor, senior, or vulnerable individual. |
| **(10)** | **Informed Consent:** | means providing consent with full understanding of the relevant facts, including risks and consequences. |
| **(11)** | **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. |
| **(12)** | **OIPC:** | means the Office of the Information and Privacy Commissioner of Alberta. |
| **(13)** | **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. |
| **(14)** | **POPA:** | means the Alberta Protection of Privacy Act. |
| **(15)** | **Synthetic Data:** | means artificial data created to maintain the structure and patterns of real data without being linked to any individual in the original data set. |
| **(16)** | **Transitory Record:** | means information that have limited or temporary usefulness. This includes auto-reply messages, routine messages, all staff email, blank forms, advertising material, and convenience or duplicate copies. |

## C. RELATED LEGISLATION

- *Alberta Access to Information Act (ATIA)*
- *Alberta Protection of Privacy Act (POPA)*

## D. RELATED DOCUMENTS

- Access Controls – Issues of Keys and Access Cards
- Access to Information Procedure
- AI Policy
- CCTV Surveillance Systems Policy
- Code of Conduct
- Data Breach of Security Policy and Procedure
- Data Quality Assurance Process
- Employee Progressive Discipline Policy and Procedure
- IT Password and Authentication Policy and Procedure
- Privacy Breach Procedure
- Privacy Policy
- 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 |