Procedure

PRIVACY BREACH 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 the process for responding to privacy incidents, including those escalated to privacy breaches, to ensure timely containment, assessment, mitigation, documentation, and notification.

This procedure works in conjunction with the Data Breach of Security Policy and Procedure for data breaches that involve data systems.

A privacy breach that does not involve a data system should be reported as per this procedure.

2. Responsibilities

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

i. Delegate duties to the Information Access & Legislative Compliance
ii. Uphold POPA
iii. Authorize the investigation of privacy issues or breaches in the event they become aware of an issue.
iv. Support and comply with the investigation process
v. Report to the Keyano Board of Governors as required

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. Support and comply with the investigation process

c. Information Technology:

i. Coordinate with the Information Access & Legislative Compliancein the event of cybersecurity incident particularly with regards to the investigation, documentation, reporting and remediation
ii. Assist in containment activities, including securing systems, disabling accounts, or isolating compromised infrastructure.
iii. Support technical analysis of the incident, including logs, access records, and system integrity reviews.
iv. Implement technical remediation actions to prevent reoccurrence.
v. Ensure security arrangements meet POPA requirements for protecting personal information and data derived from personal information.
vi. Work with Information Access & Legislative Complianceto complete mitigation and remediation measures, including system or process changes, training enhancements, and risk prevention strategies

d. People and Culture:

i. Inform Information Access & Legislative Complianceif they become aware of any suspected or actual privacy breaches in the course of any labour relations issue.
ii. Work with Information Access & Legislative Complianceto complete mitigation and remediation measures, including system or process changes, training enhancements, and risk prevention strategies

e. Records Management role and Information Access & Legislative Compliance:

i. Coordinate with Information Technology department in the event of cybersecurity incident
ii. Lead the intake, assessment, containment, investigation, documentation and resolution of all privacy incidents.
iii. Conduct preliminary and detailed risk assessments, including evaluating whether an incident meets the real risk of significant harm (RROSH) threshold under POPA.
iv. Determine if mandatory notification is required and prepare notifications to the affected individuals, the Office of the Information and Privacy Commissioner, and the Office of the Minister of Technology and Innovation.
v. Coordinate mitigation and remediation measures, including system or process changes, training enhancements, and risk prevention strategies.
vi. Maintain incident records in accordance with retention requirements.
vii. Report incidents and trends to President as Head of the Public Body
viii. Notify People and Culture if breach falls under Code of Conduct, Progressive Discipline Policy or any College policy or procedure.
ix. Liaison with the Office of the Information and Privacy Commissioner
    1. In responding to privacy breach complaints
    2. Reporting cybersecurity or privacy breaches as required under the Protection of Privacy Act.
    3. Responding to investigations or orders by the Commissioners
    4. Implementing orders from the OIPC
x. Notify law enforcement if the breach is of criminal nature.

f. Employees:

i. Fulfill duties to protect personal information in the custody and control of the College in accordance with POPA.
ii. Report any suspected or actual privacy incidents immediately to the Information Access & Legislative Compliance
iii. Support and comply with the investigation process
iv. Follow containment instructions when directed

3. Procedure

a. Identification of a Privacy Incident or Privacy Breach

i. Any employee who becomes aware of a suspected or actual privacy incident or privacy breach must immediately report it to the Information Access & Legislative Compliance.
ii. If the incident involves a data breach of security (i.e. system hack, ransomware, etc.) follow the Data Breach of Security Procedure.
iii. Reports must be made as soon as possible and include all available details, including: nature of the incident, systems or records affected, individuals potentially impacted, and time, date, and method of discovery.

b. Containment

i. Upon receiving a report, the Information Access & Legislative Compliance will immediately contain the breach. This could include stopping the unauthorized practice, recovering the records, notifying Information Technology to shut down the system that was breached or removing access to a system, or to correct a weakness in a system.

c. Preliminary Assessment

i. The Information Access & Legislative Compliance will conduct a preliminary assessment to determine if a privacy incident or privacy breach has occurred and if personal information, data derived from personal information, or non-personal information has been involved.
ii. This assessment will determine:
    1. The scope of the incident or breach
    2. The type and sensitivity of the information involved
    3. The number and identity of the affected individuals, and
    4. Whether the circumstances may create a real risk of significant harm (RROSH) requiring notification under POPA.
    5. If the assessment determines that personal information or data derived from personal information was not involved, the incident will be documented and closed.

d. Detailed Risk Assessment

i. If personal information or data derived from personal information is involved, the Information Access & Legislative Compliance will perform a detailed assessment using the risk factors as outlined in the POPA Ministerial Regulation. These include:

1. Whether there is a reasonable basis to believe that the personal information has been or will be misused.
2. Whether the loss of, unauthorized access to or unauthorized disclosure of the personal information occurred as a result of malicious intent.
3. The sensitivity of the personal information that was lost or accesses or disclosed without authorization, specifically if the information is highly sensitive information under POPA.
4. Any mitigating measures taken or other factors that reduce the risk of significant harm.

ii. The Information Access & Legislative Compliance in determining if there is a real risk of significant harm will examine if there could be bodily harm, humiliation, damage to reputation, or relationships, loss of employment, business or professional opportunities, identify theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property, or other legal harms or financial loss.

iii. The Information Access & Legislative Compliance may seek additional information from Information Technology, the individual who reported the incident, witnesses, managers, etc. to evaluate the scope or extend of the incident, risk of significant harm, and any mitigating measures.

iv. If there is no risk of significant harm, no external reporting is required. The Information Access & Legislative Compliance will complete documentation and report findings to President as Head of Public Body. Report may include recommendations to mitigate a future incident.

e. Documentation

i. All steps in the assessment and response must be documented. The Information Access & Legislative Compliance will create an Incident Summary Report detailing:
   1. The reporting of the incident
   2. Containment actions
   3. Preliminary assessment
   4. Description of incident or breach
   5. Containment actions
   6. Assessment findings
   7. Investigation notes
   8. Notifications decisions
   9. Follow up actions

ii. This documentation must be completed and maintained to demonstrate due diligence and regulatory compliance

f. Notification Decision

i. Under the POPA Ministerial Regulation, public bodies must notify affected individual, the Office of the Information and Privacy Commissioner, and the Office of the Minister of Technology and Innovation when a privacy incident or breach involving personal information creates a real risk of significant harm.

ii. Notification must occur without unreasonable delay once the risk of significant harm as been determined.

iii. If notification is required, the Information Access & Legislative Compliance will prepare and issue notices in accordance with POPA in the prescribed manner for each party.

g. Mitigation and Remediation

i. The Information Access & Legislative Compliance will coordinate remediation activities to address root causes and prevent reoccurrence.
ii. Mitigation actions may include:
    1. Revising security controls
    2. Updating processes or approvals
    3. Modifying or restricting access privileges
    4. Implementing additional safeguards
    5. Providing staff training or awareness
iii. Remediation must be proportionate to the sensitivity of the information involved and may involve People and Culture if the warranted under the Code of Conduct Policy or Employee Progressive Discipline Policy and Procedure.

h. Post-Incident and Post-Breach Review

i. Information Access & Legislative Compliance will report to President findings including details of incident, steps taken, outcomes, and recommendations or remediations.
ii. Annual reports of the Information Access & Legislative Compliance will include anonymized summarization of privacy incident and privacy breaches, trends, root causes, and recommendations or remediations steps taken.

i. Record Retention

i. The Information Access & Legislative Compliance will maintain full records of all privacy incidents and privacy breaches, regardless of whether notification was required.
ii. Records must be maintained in accordance with the Records Classification and Retention Schedule and POPA requirements.

B. DEFINITIONS

(1)	**Control:**	means the College has authority to manage, restrict, or administer the collection, use and disclosure of a record.
(2)	**Custody:**	means the College has physical possession of a record.
(3)	**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.
(4)	**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.
(5)	**Highly Sensitive Information/Data:**	means biometric information about an individual, financial information about an individual, personal information respecting a minor, senior, or vulnerable individual.

(6)	**Non-Personal Data:**	means 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 under POPA Ministerial Regulations.
(7)	**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.
(8)	**Real Risk of Significant Harm:**	means that the unauthorized access to or disclosure of personal information could cause bodily harm, humiliation, damage to reputation, or relationships, loss of employment, business or professional opportunities, identify theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property, or other legal harms or financial loss.

C. RELATED LEGISLATION

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

D. RELATED DOCUMENTS

- Code of Conduct Policy
- Cybersecurity Incident Response Plan
- Data Breach of Security Policy
- Employee Progressive Discipline Policy and Procedure
- Privacy Breach Procedure
- Privacy Policy and Procedure

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