BREACH OF PRIVACY INFORMATION REPORTING

This procedure is governed by its parent policy. Questions regarding this procedure are to be directed to the identified Procedure Owner.

Category:	B. Administration
Parent Policy:	B15
Approval Date:	May 15, 2026
Effective Date:	May 15, 2026
Procedure Owner:	Access & Privacy Coordinator

Overview:	Olds College of Agriculture & Technology (the "College") has an obligation to collect, use and disclose personal information for purposes that facilitate achieving its mandate and complying with law. The College also has an obligation to protect personal information by making reasonable security arrangements against such risks such as unauthorized access, collection, use, disclosure or destruction. This procedure outlines the actions and expectations of members of the College community regarding breaches of personal information, and privacy, and the College's duties as defined by the *Protection of Privacy Act* ("POPA").

Procedures:	A privacy breach occurs when there is a contravention of POPA through an unauthorized access to or collection, use, disclosure or disposal of personal information. Four steps will be taken to respond to a privacy breach: containment, evaluation, notification and prevention.
	
	All College employees are required to follow the Privacy Breach Reporting Procedure in the event of a breach involving personal information. Employees must contact the Access & Privacy Coordinator immediately if they suspect that a privacy breach has occurred.
	
	Identifying a Breach
	There are five types and causes of breaches:
	
	• **Technical Problem**
	  • Data leak
	  • Untraceable technical error
	• **Human Error - Accidental Disclosure or Loss**
	  • Unauthorized access or disclosure (e.g. misdirected email)
	  • Loss of physical devices or documents containing personal information
	• **Theft**
	  • Stolen physical devices or documents containing personal information

- **Malice**
  - Unauthorized access by malicious actors
- **Awareness**
  - Absent or inadequate policies & procedures
  - Absent or inadequate employee training

When a breach of personal information is suspected, the employee involved and/or the employee reporting the breach (for example, the employee who discovered the breach) will work with their Supervisor and the Access & Privacy Coordinator as outlined in this procedure. If the Access & Privacy Coordinator determines a breach of personal information did not occur, they will notify the business area in writing of their findings.

Step 1 - Containment

- Immediate containment of the record(s) must swiftly be undertaken. This includes recalling internal email messages and notifying all recipients:
  a. that they received it in error;
  b. to advise not to open and/or distribute the record; and
  c. to destroy the information including from their downloaded files and recycle bin.
- The employee responsible for the custody and control of the information at the time of the breach must preserve a copy of the evidence of the breach and notify the Access & Privacy Coordinator within one working day after becoming aware of the incident. If the incident is not reported within one working day, a reason for the delay must be communicated to the Access & Privacy Coordinator.
- The Access & Privacy Coordinator will initiate the Privacy Breach Reporting Process as outlined in the reporting form, within two working days upon receipt of notification of the incident.

Step 2 - Investigation and Evaluation

The breach will be evaluated through the information supplied by the business area via the Privacy Breach Reporting Form to determine if the event requires notification to internal and/or external stakeholders. The evaluation process is independent and will be led by the Access & Privacy Coordinator to determine if a breach of personal information occurred under POPA. Evaluation will include determining the number of affected individuals, if notification to external regulatory bodies will be required, the intentional or unintentional nature of the breach, and overall risk.

Step 3 - Notification

The business area, or the Access & Privacy Coordinator if the breach is large in scope and overall risk, must notify the affected individual(s) of the breach as soon as possible from the date the breach was discovered. Notification should include:

1. A description of what happened;
2. What information was involved;
3. What is being done to prevent a similar breach in the future;
4. What the affected individual(s) can do (e.g. changing their passwords), if possible, to mitigate the likelihood of the risk;
5. Who to contact for more information (Access & Privacy Coordinator);
6. The individual's right to contact the Office of the Information and Privacy Commissioner (OIPC), including the OIPC's contact information.

Step 4 - Prevention

1. Once the Privacy Breach Reporting Form is returned to the employee reporting the incident, it must be signed by all required parties and returned to the

OLDS COLLEGE
OF AGRICULTURE & TECHNOLOGY

	Access & Privacy Coordinator as soon as possible, but no later than 10 working days, from the time the original form was sent to the business area. 2. The business area responsible for the breach must also undertake and implement any required physical, technical and/or administrative safeguards as recommended by the Access & Privacy Coordinator in the Privacy Breach Reporting Form. 3. The Access & Privacy Coordinator will follow up with the business area three months after the close of the breach for a status update on any required changes to improve safeguards. All employees are expected to be aware of and uphold their obligations under the POPA as reflected in College policy and procedure.
Definitions:	**Employee:** includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body.
	Personal Information: means information about an identifiable individual including, but not limited to:' ● Name, home or business address, home or business telephone number home or business email address, or other contact information* ● Race, national or ethnic origin, color or religious or political beliefs or associations ● Age, gender, identity, sex, sexual orientation, marital status or family status ● An identifying number, symbol or other particular assigned to an individual ● Fingerprints, other biometric information, blood type, genetic information or inheritable characteristics ● Health and health care history, including information about physical or mental health ● Educational, financial, employment or criminal history ● Anyone else's opinion about the individual ● An individual's personal views or opinions, except if they are about someone else *NOTE: Business contact information is a type of personal information that is routinely disclosed in a business or professional context. The disclosure of business contact information, in and of itself, is not usually an unreasonable invasion of privacy
	Privacy Breach: means a loss of, unauthorized access to or unauthorized disclosure of personal information.
Related Information: * link to access to legislation	*Protection of Privacy Act* *Protection of Privacy Act (Ministerial) Regulation* *Protection of Privacy Act Regulation* Privacy Breach Reporting Form
Review Period:	3 years
Revision History:	New: February 2024 Revised: April 2026