BREACH OF PERSONAL 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:	B04
Approval Date:	February 9, 2024
Effective Date:	February 9, 2024
Procedure Owner:	FOIP 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 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, the protection of privacy and the College's duties as defined by the Alberta *Freedom of Information and Protection of Privacy (FOIP) Act.*

Procedures:

A privacy breach occurs when there is a contravention of the FOIP Act 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 FOIP Coordinator immediately if they suspect that a privacy breach has occurred.

Identifying a Breach

There are six main types of breaches:

1. **Human Error - Accidental Disclosure** (e.g. misdirected email)
2. **Human Error - Accidental Loss** (e.g. loss of physical devices or paper containing personal information)
3. **Theft** (e.g. stolen physical devices or paper containing personal information)
4. **Malicious** (e.g. unauthorized access by malicious actor(s)
5. **Data Leak** (e.g. breach of College policy and/or procedure)
6. **Technical** (e.g. untraceable technical error)

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 the FOIP Coordinator as outlined in this procedure. If the FOIP Coordinator determines a breach of personal information did not occur, they will notify the business area in writing of their findings.

Step 1 - Containment

In the event a breach or suspected breach involving personal information occurs:

1. 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.
2. 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 FOIP 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 FOIP Coordinator.
3. The FOIP 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 - Evaluation

The breach will be evaluated through the information supplied by the business area and/or 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 FOIP Coordinator to determine if a breach of personal information occurred under the FOIP Act. 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 FOIP 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; and
5. Who to contact for more information (e.g. FOIP Coordinator).

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 FOIP Coordinator as soon as possible 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 FOIP Coordinator in the Privacy Breach Reporting Form.
3. The FOIP Coordinator will follow up with the business area three months after the close of the breach for a status update on required changes to improve safeguards.

	All employees are expected to be aware of and uphold their obligations under the FOIP Act as reflected in College policy and procedure.
Definitions:	**Employee:** under the FOIP Act and for the purposes of this procedure, an employee includes 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. **Personal Information:** The recorded information about an identifiable individual, including: • The individual's name, home address or telephone number; • The individual's race, national or ethnic origin, colour or religious or political beliefs or associations; • The individual's age, sex, marital status or family status; • An identifying number, symbol or other particular assigned to the individual; • The individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics; • Information about the individual's health and health care history, including information about a physical or mental disability; • Information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given; • Anyone else's opinions about the individual; and • The 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 as per section 40(1)(bb.1) of the FOIP Act. **Privacy Breach:** means a loss of, unauthorized access to, or unauthorized disclosure of personal information.
Related Information:	B04 Access to Information Procedure B04 Protection of Privacy Procedure FOIP Notification Statement Privacy Breach Reporting Form FOIP Request to Access Information Form *Freedom of Information and Protection of Privacy Act* *Post-Secondary Learning Act*
Review Period:	3 years
Revision History:	New: February 2024