OLDS COLLEGE
OF AGRICULTURE & TECHNOLOGY

Privacy Management Program Framework

REV. MAY 5, 2026

TABLE OF CONTENTS

INTRODUCTION

Olds College of Agriculture & Technology's (the College's) *Privacy Management Program Framework* reflects the College's commitment to achieve compliance with the *Protection of Privacy Act* ("POPA") and the *Access to Information Act* ("ATIA"). The College commits to earn and maintain trust by exceeding privacy requirements prescribed by legislation and be transparent about the College's internal governance structures and privacy practices.

This *Privacy Management Program Framework* is intended to supplement the College's Privacy Policies and Procedures by providing more in-depth information about the College's internal key practices related to the collection, use, disclosure, retention and protection of personal information designed to achieve the following five (5) purposes set out in the Acts:

- A right of access to records
- Protection of personal privacy
- A right of access to an individual's own personal information
- A right to request a correction
- Independent review of a decision

The *Privacy Management Program Framework* is divided into three parts:

1. The Olds College Privacy Commitment
2. Privacy Controls and Practices
3. Privacy Monitoring and Improvement

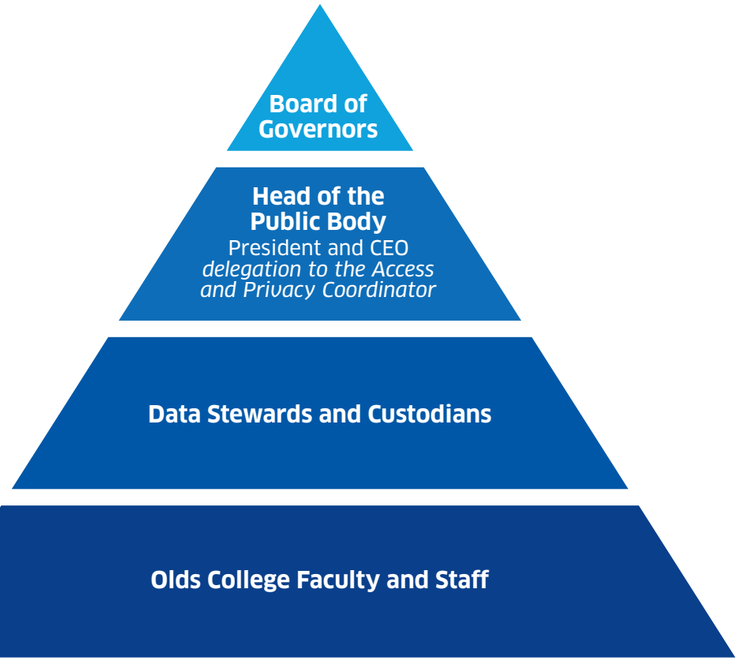
Each part of the *Privacy Management Framework Program* describes core privacy practices and processes, and provides operational privacy tools, such as templates, guides, forms, tip sheets and reference to additional resources, in an effort to be transparent about how Olds College handles personal information and to assist Olds College employees in establishing and maintaining good privacy practices across the organization.

PART 1:

OLDS COLLEGE OF AGRICULTURE & TECHNOLOGY PRIVACY COMMITMENT

ORGANIZATIONAL STRUCTURE

Olds College has a governance structure in place to ensure compliance with POPA and ATIA and to promote the College's *Privacy Management Program Framework:*



Key Partnerships

To effectively manage privacy, key partnerships within Olds College are essential. The College's *Privacy Management Program Framework* relies on collaboration with the following key partners:

- Executive Offices
- Institutional Research and Program Development
- Data Stewards and Custodians
- People and Culture
- Information Technology
- Office of the Registrar
- Academic Schools
- Office of Research Services

PART 2:
PRIVACY CONTROLS AND PRACTICES

A. LEGISLATION AND POLICIES

Legislation

Alberta's Protection of Privacy Act and ***Access to Information Act*** together set out the following purposes:

- **A right of access to records** in the custody or under the control of a public body subject to limited and specific exceptions as set out in the *Access to Information Act*.
- **A right of access to an individual's own personal information,** subject to limited and specific exceptions as set out in the *Access to Information Act*.
- **A right to request a correction** to an individual's personal information, subject to limited and specific exceptions as set out in the *Access to Information Act*.
- **Protection of personal privacy** by controlling the manner in which a public body may collect, use and disclose personal information.
- **Protection of personal privacy** by controlling the creation, use and disclosure of data derived from personal information and non-personal data.
- **Independent review of decisions** made by a public body under the Protection of Privacy Act and the Access to Information Act and for the investigation of complaints. Independent review is provided by the Office of the Information and Privacy Commissioner ("OIPC") of Alberta.

The *Protection of Privacy Act* further provides that the head of the public body must protect personal information by making reasonable security arrangements against any risks, including unauthorized access, collection, use, disclosure or destruction of personal information.

Policies

Olds College has a number of privacy-related policies, developed collaboratively across the organization, focused on ensuring compliance with the Acts and alignment with sector best practices:

- Access to Information Policy
  - ◇ Access to Information Procedure
- Protection of Privacy Policy
  - ◇ Protection of Privacy Procedure
  - ◇ Privacy Breach Procedure
  - ◇ Privacy Impact Assessment Procedure
- IT Governance and Technology Management Policy
  - ◇ Acceptable Use IT Standard
  - ◇ Digital Security Procedure
  - ◇ Institutional Data Governance Procedure
    - ▪ Security Classification Procedure
  - ◇ IT Governance and Technology Management Procedure
- Records Management and Disposition Policy
  - ◇ Records Management and Disposition Procedure

Olds College administrative policies are approved by the College Leadership Team on the recommendation of the Policy and Procedure Review Committee. Administrative policies are available to College faculty, students, staff and the public.

B. DIRECTORY OF PERSONAL INFORMATION BANKS

The College's new digital *Directory of Personal Information Banks* will bring Olds College into compliance with the *Protection of Privacy Act* and promote transparency about the types of personal information collected, reasons for collection and how the personal information will be used by the College.

The *Directory of Personal Information Banks* includes, for each Personal Information Bank, the following:

- The title and location of the personal information bank.
- The authority for collecting the personal information.
- A description of the type of personal information and the categories of individuals whose personal information is included.
- The purposes for which the personal information was collected or compiled and the purposes for which it is used or disclosed.

OPERATIONAL PRIVACY TOOLS

- Personal Information Bank Guide
- Personal Information Bank Template

DIGITAL TOOLS FOR PERSONAL INFORMATION BANKS

A digital library that tracks and publishes a *Directory of Personal Information Banks* across the organization, effective June 11, 2026, to provide College employees, students and the public with information about the College's personal Information holdings and uses, and to assist individuals with exercising their access and correction rights under the *Protection of Privacy Act*.

C. ACCURACY AND ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

The *Protection of Privacy Act* provides individuals with a right of access to records in the custody or under the control of the College, subject to limited and specific exceptions set out in the legislation; and with a right to request corrections to their personal information about them held by the College. When the College receives an access to information request, it follows a consistent process for providing access to information:

1. Applicant requests information.
2. Request for records is sent to applicable departments.
3. Each record is reviewed line-by-line; limited and specific exceptions may apply to disclosure.
4. Response is provided within 30 business days unless a time extension is agreed upon.

Access to information requests provide individuals with access to two different types of records in the custody or under the control of the College:

General Information
is recorded information not about an identifiable individual.

Personal Information
is recorded information about an identifiable individual.

Members of the public and College employees and students who wish to access and/or correct their personal information can complete the College's **Access to Information Request Form** or the **Request to Correct Personal Information Form.**

OPERATIONAL PRIVACY TOOLS

- Access to Information Request Form
- Request to Correct Personal Information Form

D. COLLECTION OF PERSONAL INFORMATION

Section 4 of the *Protection of Privacy Act* provides that no personal information may be collected by or for a public body unless:

- The collection of that information is expressly authorized by an enactment of Alberta or Canada.
- That information is collected for the purpose of law enforcement.
- That information relates directly to and is necessary for an operating program or activity of the public body.

Personal information must be collected only in accordance with the provisions of the *Protection of Privacy Act*. The College's Protection of Privacy Policy and Procedure provides information on why the College collects personal information, when it collects personal information, as well as a list of examples. The *Protection of Privacy Act* sets the rules on how the College collects personal information:

Minumum Collection

The College only collects the minimum amount of personal information required for the operating program or activity of the College.

Direct Collection

The College only collects personal information directly (some exceptions may apply under the *Protection of Privacy Act.)*

Direct Collection of Personal Information - Notice

When collecting personal information, a notice of collection is provided informing individuals of:

A. The purpose for which the information is collected.

B. The specific legal authority for the collection.

C. The title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Notice is given prior to collection and may be given in manners appropriate to the situation and context. Generally, notice is provided on College forms, brochures, handouts, on posters in public areas and anywhere information is collected electronically. In certain circumstances, it may be provided verbally.

The College is committed to consistency across all College departments and programs in order to help College employees, students and the public receive similar notices no matter where collection occurs with the College.

OPERATIONAL PRIVACY TOOLS

- Standard collection notification
- Access to *Employee Access and Privacy Quick Reference Guide*

E. RETENTION AND DISPOSITION OF PERSONAL INFORMATION

The *Protection of Privacy Act* provides that if an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must retain the personal information for at least one year after using it to make a decision, so that the individual has a reasonable opportunity to obtain access to it, or for any shorter period of time as agreed to in writing by:

A. The individual.

B. The public body.

C. If the public body that approves the records and retention and disposition schedule for the public body is different from the public body, that body.

Retention

Managing records disposition is part of the College Records and Information Management Program. The College's mandate is to retain College records until they have met operational, legal, fiscal and archival requirements as set out in the Records Retention Schedule. This is an important part of ensuring that retention schedules are adhered to in order to retain personal information only for the amount of time that is required for operational, legal, fiscal and/or archival purposes.

Disposition

Corporate records are retained until they have met operational, legal and fiscal value to the College, at which time they are disposed of by destruction, deletion or transfer to the College's archives. This disposition process ensures that corporate records are retained and disposed of in accordance with the Records Retention Schedule, and ensures the appropriate handling of confidential materials and the transfer of records designated for permanent preservation to archives. Disposition of records may be delayed or suspended as a result of an audit, a legal action, a change in legislation, an access to or correction of information request, or a change in the use of a record or record series.

When records have met their retention requirements, the disposition process is implemented. Disposition of records requires the appropriate approvals and sign-off as outlined in the College's Records Management and Disposition Procedure. This administration policy also ensures that any destruction carried out in accordance with the Records Retention Schedule is appropriate for the type of record, and that appropriate security measures are observed for the disposition of records containing personal or other confidential information.

F. PROTECTION OF PERSONAL INFORMATION

The *Protection of Privacy Act* requires that the head of a public body must protect personal information by making reasonable security arrangements against such risks as:

- unauthorized access
- collection
- use
- disclosure
- destruction

Physical

Access and authorization mechanisms (for example, employee access cards) are in place to limit access to only authorized individuals. Physical Security Risk Assessments are completed on priority sites and physical security systems are in place to protect sites and information assets. Secure filing rooms and cabinets are provided for personal information storage which include access control mechanisms.

Technological

The College's information assets are controlled and protected. With the extensive use of technologies, services and tools, we provide:

- access controls on devices
- access control for applications and databases
- risk management
- intrusion protection
- usage restrictions
- virus protection
- network security
- multi-factor authentication

Administrative

College employees and third parties contracted by the College have access to administrative policies, including Privacy Impact Assessments, and training to bring awareness to their responsibilities related to information management, security and privacy. Our administrative policies identify roles and responsibilities, as well as provide direction to staff on how to protect personal information. Resources are in place to support information sharing with suppliers, vendors and contractors, including contractual obligations stipulating confidentiality and security of information, as well as privacy breach protocol.

F. PROTECTION OF PERSONAL INFORMATION

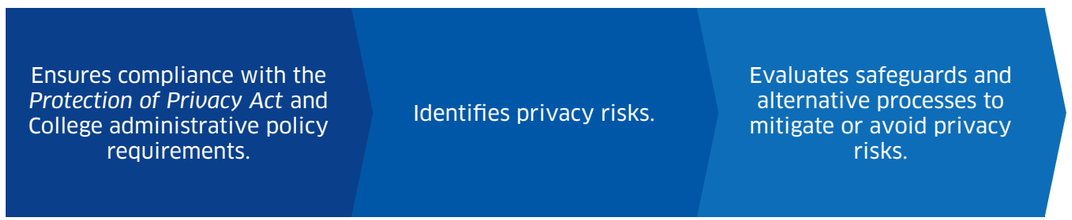
Essential to the College's commitment to protect personal information of stakeholders, students, staff and faculty, and making reasonable security arrangements against unauthorized access, collection, use, disclosure or destruction, is identification and mitigation of privacy risks in any new or substantial change to an existing project, process, initiative and information technology.

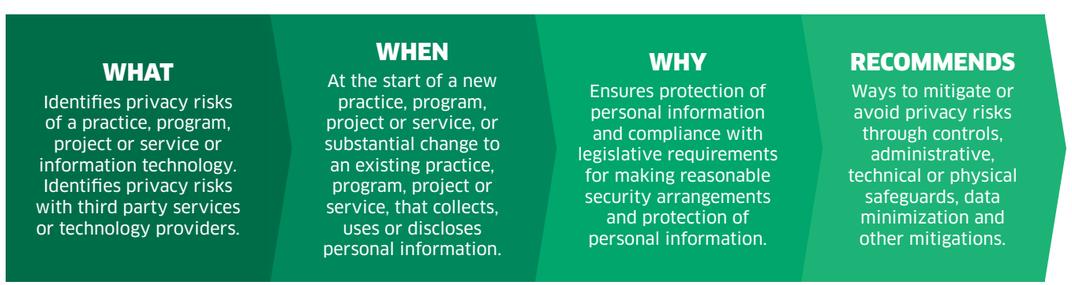
New services undergo cybersecurity and privacy assessments prior to implementation. Olds College uses the Higher Education Community Vendor Assessment Toolkit (HECVAT) to evaluate services that may impact private data. As part of the process, vendor SOC 2 reports are reviewed to assess security controls, privacy safeguards and overall risk to institutional and personal data.

The College's primary tool for identifying privacy risks is a Privacy Impact Assessment ("PIA"). Under the *Protection of Privacy Act,* the College must prepare a PIA with respect to a "new or a substantial change to an existing, administrative practice, program, project or service that involves the collection, use or disclosure of personal information" if:

1. The loss of, unauthorized access to or unauthorized disclosure of the personal information could result in significant harm; OR
2. If the practice, program, project or service:
   a. will collect, use or disclose personal information deemed to be of high sensitivity.
   b. will involve the personal information of a significant percentage of the population we serve.
   c. will involve data matching with another public body.
   d. is part of a common or integrated program or service.
   e. involves the development or use of innovative technology.

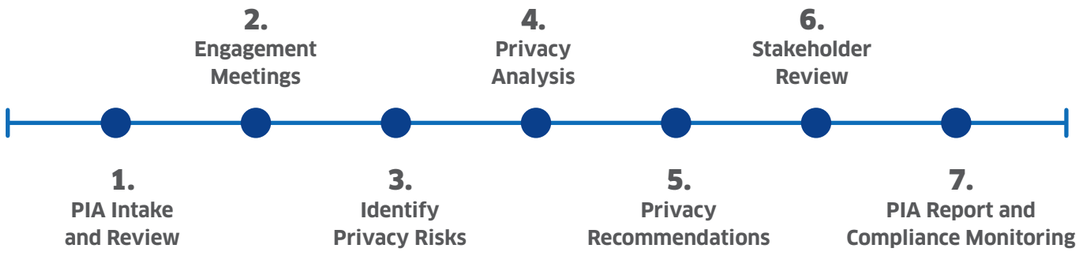
The College's administrative procedure requires that all practices, programs, projects or services that involve the collection, use or disclosure of personal information undergo a PIA. A PIA helps facilitate Privacy by Design and builds privacy directly into the College's practices and technologies at the outset and not as an afterthought. A PIA:





F. PROTECTION OF PERSONAL INFORMATION

The Privacy Impact Assessment ("PIA") Process



OPERATIONAL PRIVACY TOOLS

- PIA Assessment Guide
- PIA Template
- Privacy Fact Sheet: Privacy Impact Assessments
- Privacy Impact Assessment Procedure

DIGITAL TOOLS FOR PERSONAL INFORMATION BANKS

A digital library that tracks and manages PIAs for College administrative practices, programs, projects or services involving personal information collection, use and disclosure is available on the OC Connect Access and Privacy page.

A complete list of accepted PIAs since July 1, 2026 are available on oldscollege.ca, providing the public with information about how the College handles their personal information in College administrative practices, programs, projects, services and technologies.

H. PRIVACY BREACH MANAGEMENT

The College is committed to safeguarding personal information and making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

There may be times when the College's reasonable security safeguards (administrative, technical and/or physical) may be compromised, inadequate, missing or subject to malice, and a privacy breach occurs. A privacy breach means a loss, unauthorized access to or disclosure of personal information. The College's definition of privacy breach is aligned with that of the Office of the Information and Privacy Commissioner (OIPC) of Alberta. Generally, privacy breaches can occur as a result of:

The College has mechanisms in place to:

- Enable stakeholders, students and staff to raise privacy concerns regarding compliance with the *Protection of Privacy Act* or the College's privacy practices.
- Bring awareness to College employees' requirement to report all privacy concerns, including suspected privacy breaches.
- Take urgent action to contain, investigate, notify and prevent future privacy breaches.

H. PRIVACY BREACH MANAGEMENT

Privacy Breach Response Process

1. Contain

Once a privacy breach has been identified, it is important to take immediate actions to contain the privacy breach, if possible, and notify a Supervisor and the Access and Privacy Coordinator. This step ensures that any potential or real harm to the affected individual(s) or others is minimized. The Access and Privacy Coordinator will assist departments in containing the privacy breach and will coordinate with key partners, when required. If the privacy breach is a result of theft or other criminal activity, departments should notify the Olds RCMP Service.

2. Investigate and Evaluate

The breach will be evaluated through the information supplied via the Privacy Breach Reporting Form. The form collects the following information, and supporting evidence may be required, to aid with an investigation into a privacy breach:

- Incident description
- Personal information involved
- Safeguards
- Harm
- Risk assessment
- Containment
- Notification (if necessary)

The investigation process determines what other actions are needed. An evaluation of risks associated with a privacy breach is always completed, including but not limited to:

- Personal information elements involved?
- Scope and number of affected individuals?
- Cause and extent of the privacy breach?
- Possible harm?

Members of the public, College employees and students also have the right to notify the Alberta OIPC. If a privacy complaint is investigated by the OIPC, the College fully cooperates with the Information and Privacy Commissioner's investigation.

3. Notify

The *Protection of Privacy Act* requires that if an incident occurs involving the loss of, unauthorized access to or unauthorized disclosure of personal information in the custody and control of the College, where a real risk of significant harm exists, the College must, without reasonable delay, give notice of the incident to:

- The individual(s) to whom there exists a real risk of significant harm.
- The Information and Privacy Commissioner.
- The Minister.

The Access and Privacy Coordinator will work with the affected department to prepare and deliver the required notifications.

Notification to an Affected Individual(s)

Content of the College's notification to affected individual(s) will vary depending on the nature of the privacy breach and the method of notification.

- Date of the privacy breach.
- Description and general circumstances of the privacy breach.
- Description of the personal information involved in the privacy breach.
- The steps the affected individual(s) can take to further mitigate the risk of harm.
- Contact information for the College's Access and Privacy Coordinator who can answer questions.
- The individual(s) have a right to contact the OIPC, including the OIPC's contact information.

Generally, notification is provided by the College's Access and Privacy Coordinator directly to the affected individual(s) in writing; however, there may be circumstances where indirect notification is given via oldscollege.ca, posted notices or by the Communications Department.

H. PRIVACY BREACH MANAGEMENT

4. Prevent and Audit

Following containment, investigation and evaluation, time is taken to thoroughly analyze the privacy breach and develop recommendations with respect to what measures and/or safeguards could be taken to prevent future privacy breaches. Recommendations can include, but are not limited to:

- Discontinuation of current practices.
- Business process changes, including completing a Privacy Impact Assessment.
- Access and Privacy Awareness Training.
- Policy and procedure development.

The resulting Letter of Findings, containing the recommendations to mitigate against future privacy breaches, includes an auditing requirement to ensure that the preventative strategies or safeguards have been fully implemented.

The roles and responsibilities with respect to managing the privacy breach response at the College are defined as follows:

Affected department

- Review privacy complaint reports.
- Implement containment measures to limit privacy breach.
- Advise the Access and Privacy Coordinator.
- Investigate and evaluate privacy breaches.

Access and Privacy Coordinator

- Review privacy compliant reports.
- Review breach reports.
- Make decisions and issues notification to affected individual(s) and/or the OIPC.
- Establish a Privacy Breach Response Team (if required).
- Offer privacy breach mitigation recommendations to departments.
- Complete a “Letter of Findings” in consultation with the affected department.
- Conduct compliance audit reviews.

Data Stewards and Custodians

- Assist respective departments in reporting, containing and preventing a privacy breach, including suspected privacy breaches.

Head of the Public Body

- Maintains overall accountability for privacy breach response.
- Escalates privacy breach matters to Executive Leadership and the Board of Governors.

Privacy Response Team

Depending on the circumstances of the privacy breach, a privacy breach response team may be established to carry out containment, notification and to minimize any current, ongoing or future risks associated with a privacy breach.

Membership of the privacy breach response team varies depending on the context, and may include:

OPERATIONAL PRIVACY TOOL KIT

- Privacy Complaint Report Forms
  - ◇ Members of the public
  - ◇ College employees
- OIPC POPA Breach Notification Form
  - ◇ POPA Breach Notice Assessment Tool

I. USE OF THIRD-PARTY SERVICES OR TECHNOLOGIES

Third-Party Protection of Personal Information

The College may engage third-party service providers to supply a service which is managed by the College. In these instances, the third-party service provider is an 'employee' of the College, and as such, has a duty under the *Protection of Privacy Act* to protect the personal information that it collects, uses and discloses as part of that service. Privacy awareness training is available to third-party providers.

By engaging in the PIA process when selecting service providers, the College can ensure service providers limit the collection of personal information, have adequate safeguards in place to protect the personal information it collects, uses and discloses on behalf of the College, and will dispose of the personal information after the business purpose for the collection has been completed.

Data Protection of Personal Information

Information security design is part of all systems and infrastructure architecture design; information technology technical processes, business practices and methodologies follow College policies and standards; and plans for business continuity are in place. All data located on College websites and in email, software applications, databases, files (documents, spreadsheets, images, etc.) and other information repositories supported by Information Technology are managed, protected and monitored. Third-party technologies provide, but are not limited to:

- Email protection from spam and malware
- Secure processing of financial transactions
- Reporting and alerts
- Various means of restricting changes to our systems
- Secure web traffic transmission and protection of files

User Authentication

Systems and procedures are in place to authenticate users. The College requires user name and a unique password or two-factor authentication before access is granted to systems handling personal information.

Device Management

Information Technology uses tools to manage the College's desktop and laptop computers which provide standardization for how they are built and installed, hard drive encryption, enforcement of security rules and regularly updated security patches.

To help ensure business continuity and protection of data, Information Technology keeps the College's technologies and services up to date and stable to ensure the latest security protections are in place. This includes operating systems, servers, databases, computers and mobile devices, as well as the College's wired and wireless networks.

College administrative policies restrict the use of unapproved hardware and software for storing personal information. This includes personal devices, removable media (thumb drives) and hosted software without appropriate identity management and authentication.

Change Control

Information Technology maintains a change control process which ensures that new implementation and modifications to systems follow strict change control processes to ensure system data is not exposed.

J. AWARENESS, EDUCATION AND TRAINING

4. Prevent and Audit

The College believes that everyone in our organization has a role to play in protecting personal information. College employees receive training on privacy and reporting privacy complaints. The College is committed to ensuring our employees have access to training and development to protect personal information when developing administrative practices, programs, projects or services, and when handling personal information of the public, students and staff.

As part of the College's commitment to fostering a culture that respects privacy, we deliver training such as the following to raise privacy awareness amongst employees:

- Olds College onboarding
- Code of conduct
- Privacy awareness training
- Access to information training
- Cybersecurity training
- Employee Access and Privacy Quick Reference Guide

PART 3:

PRIVACY MONITORING AND IMPROVEMENT

K. MONITORING

Monitoring and reviewing the privacy practices set out in the *Privacy Management Program Framework* is important to ensure they remain relevant, effective and contribute to ongoing compliance and accountability. The College is currently monitoring the following privacy practices:

TRAINING

Relevance and best practices

Depth and breadth of content for various audiences

Build a culture of privacy at the College

PRIVACY IMPACT ASSESSMENTS

Completion of PIAs as required under legislation

Internal and public repository of PIAs

PRIVACY PROTECTION

Implement email retention rules

Annual program training, awareness and data retention

Privacy Program Control	Current Status of Privacy Program Control	Current Monitoring Frequency
Policies	Individual policies and procedures in place or under development	ongoing
Directory of Personal Information Banks	Implementing in 2026/27	annual
Risk Assessment Tools: Privacy Impact Assessments	Implementing in 2026/27	annual
Training and educational requirements	In place	annual
Privacy Complaint Management	In place	annual
Service Provider Management, including use of third-party services or technologies	In place	as needed
Communication	Implementing in 2026/27	as needed

L. IMPROVING PRIVACY PRACTICES

The College is committed to creating a culture of continuous improvement, and encourages input from College employees, students, the public and privacy experts on the College's *Privacy Management Program Framework.* In response to new *Access to Information* and *Protection of Privacy* Legislation, the College reviewed key privacy practices, privacy vision and privacy principles. The outcomes of this review, along with the recommendations of privacy experts, will be used to refine, enhance and improve current privacy practices and tools in the years ahead.

The *Privacy Management Program Framework* will be reviewed on an annual basis commencing in 2027. Each year, an oversight and review plan will be created to monitor, assess and evaluate the following:

- Privacy program controls and update as required.
- New opportunities for continuous improvement.
- Evolving information technologies, and new risks or threats to privacy.
- Provincial, national and international best practices related to privacy.

OLDS COLLEGE
OF AGRICULTURE & TECHNOLOGY

1.800.661.6537 | info@oldscollege.ca

oldscollege.ca