INSTITUTIONAL DATA GOVERNANCE

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

Category:	C. Campus Infrastructure
Parent Policy:	C04
Approval Date:	December 9, 2025
Effective Date:	December 9, 2025
Procedure Owner(s):	Director, Institutional Research & Program Development

Overview:

The Institutional Data Governance procedure establishes a set of guidelines to facilitate data management and governance across Olds College of Agriculture & Technology (the "College"). This includes:

- Overarching administrative data management and governance guidelines;
- Clarifying responsibilities and accountability for the management of College data via specific institutional roles and responsibilities;
- Supporting data integrity, validity, reliability and security;
- Facilitating data sharing, collaboration and transparency across Departments;
- Ensuring alignment to digital records retention and access to information legislation and policies;
- Enhancing data and systems coordination, process optimization and integration support; and,
- Addressing emerging data and related systems issues.

All systems or applications that contain administrative data (excluding applied research data) fall under the Institutional Data Governance procedure.

Procedures:

Data & Systems Management Roles and Responsibilities

The College will establish and manage institutional data with an emphasis on data stewardship, integrity and collaboration. Subsequently, the following roles (and associated responsibilities) have been established to promote the access, integrity and security of institutional data.

1. Data Trustees: This is an oversight role. Trustees are the highest ranking individuals accountable for data management policies as a whole. They have overall responsibility for what happens to institutional data under their oversight. Data definitions and other data related processes are approved by these individuals, and they oversee the implementation of these initiatives among respective College Departments. This includes members of the College Leadership Team (CLT); including Deans and Directors.

2. Institutional Data Steward: Institutional data stewards define the data, and create processes and procedures for core data environments (i.e. Financial, academic and human resource data). They also maintain data quality in accordance with the policies created by Data Trustees and ensure compliance and security of data for their respective environment (e.g. Staff with oversight over a specific data environment).
3. Departmental Data Steward: Departmental stewards are the managers (or designate) within a Department responsible for ensuring that data policies and standards turn into practices within their business unit. Data stewards assist the enterprise in leveraging domain data assets to full capacity. Departmental data stewards are usually the individuals who understand the data in their department better than anyone else in the organization (e.g. Department administrative staff).
4. Data Custodian: This responsibility rests with the Information Technology Department. Data custodians are responsible for safe custody, transport, storage of the data and implementation of associated business rules.
5. Data Users: Employees, students, partners, or guests of the College, who work directly with College data.

Data Governance Standards

To support effective data collection, analysis, reporting and sharing practices at Olds College, the following data management standards will apply to all College departments:

1. Data Inventory, Classification, & Definitions: Institutional Data Stewards will ensure a Data Dictionary is in place, to classify key data management and performance metric terms; including definition, data collection process, how data is to be interpreted, appropriate use/access/reporting, etc.
2. Data Management Accountabilities & Roles: College departments will designate an applicable Department Data Steward to be responsible for ensuring data policies and standards are adhered to within their respective area; and they align with procedures developed by Institutional Data Stewards.
3. Data Integrity: Institutional Data Stewards will actively manage the quality of data. This includes ensuring institution-specific standards for data quality, validity, and access are monitored to safeguard data integrity; including identifying and correcting data issues as they arise (in concert with applicable Department Data Stewards).
4. Data Security: College Departments will align with Information Technology security requirements in order to safeguard data from inappropriate use.
5. Information Technology & Data Committee Participation: As a means of supporting data management, integrity and access, Institutional Data Stewards, Data Custodians, and Data Trustees (or designates) will participate in the Information Technology & Data Committee. As per Policy C04: IT Governance and Technology Management. Terms of Reference per IT Governance & Technology Management Procedure.
6. Data Management Issue Resolution: Data issues that have the potential to impact multiple Departments and operations will be brought to the attention of the Information Technology & Data Committee, by the applicable Data Steward, for review and resolution.

Institutional Data Management Guidelines

General Data Guidelines

The following general data guidelines apply across the institution, and are meant to provide core best practices to support the secure, effective and efficient utilization

of data at the College:

1. Wherever possible, data should be collected, entered and maintained once, at the source, and made available to all members of the institution that have a business need; ensuring alignment with the *Access to Information Act (ATIA)* and the *Protection of Privacy Act (POPA);* and applicable College policies.
2. It is the responsibility of every data user to understand the data they use, inform the Data Stewards of any data issues, and to guard against making misinformed or incorrect interpretations of data.
3. Institutional data must not be accessed or manipulated for personal gain, or out of personal interest or curiosity.
4. Data users must carry out all tasks related to the creation, storage, maintenance, classification, use, protection, dissemination and disposal of institutional data responsibly, in a timely manner and with the utmost care and in compliance with applicable College policies.
5. Data users must not knowingly falsify data, delete data that should not be deleted or reproduce data that should not be reproduced.
6. Data Stewards will be responsible for defining and monitoring data quality standards to reduce risk and improve data reliability.
7. Institutional data will align with the following *Olds College Data Classification Standard* categories:
    a. Public Data:
        i. Non-proprietary information that is created in the normal course of business that is unlikely to cause harm. It is available to the general public.
    b. Protected:
        i. Protected information may include business information about how we effectively operate and conduct business as well as non-personal information.
        ii. Access limited to individuals (employees and contractors, sub-contractors and agents) possessing a need to know for business-related purposes (role-based access). Information that should be appropriately secured and not accessible by the public.
    c. Confidential:
        i. Personal information that includes data not publicly available, financial information or sensitive information uniquely assigned to an individual, personal health related information. Details concerning the effective operation of Olds College. Business or financial/business information provided to the College in confidence.
        ii. Access and/or ability to input or change the information should be limited to individuals in a specific function, group or role, for business-related purposes.
    d. Restricted:
        i. Information whose loss, corruption or unauthorized disclosure would severely harm the company's reputation or business position resulting in financial, reputation or legal loss. Access is specific to a named individual and is very limited. Information that would require the explicit approval of the information owner to release this information, even to those with a need to know.

Data Access Guidelines

The following data access guidelines specify how data is to be shared internally

and externally:

1. Institutional data must be used only by those persons duly authorized to access and use the data by virtue of their position at the College, and only for the purpose for which use has been authorized.
    a. The determination of authorized users is dependent on the *Olds College Data Classification Standard* categories; and the discretion of the applicable Data Trustees and Institutional Data Stewards.
    b. For authorized users, institutional data should be readily accessible to authorized users to view, query or update.
2. Access to institutional data for research purposes may be granted by the appropriate Institutional Data Steward, in consultation with their Data Trustee.
    a. If approved, its use is subject to College policies on privacy, security, as well as to all applicable provincial and federal privacy legislation.
3. External users accessing data must comply with the *Access to Information Act (ATIA)* and the *Protection of Privacy Act (POPA)*; and applicable College policies.

Artificial Intelligence (AI) - Administrative Data Guidelines:
Artificial intelligence tools are often utilized for a range of administrative activities, including writing and editing documents and emails, brainstorming, summarizing information, and addressing questions. These tools can fulfill a valuable role for the institution, however they do require awareness of privacy and operational realities. The following guidelines provide guidance on the effective use of AI-based tools within the College environment:

Artificial Intelligence General Guidelines:

1. The use of any institutional data within Artificial Intelligence (AI) or machine learning applications must comply with the *Access to Information Act (ATIA)* and the *Protection of Privacy Act (POPA)*; and applicable College policies.
2. Olds College leverages the "*FASTER*" Artificial Intelligence governance principles developed by the Government of Canada to inform general AI activities.

Government of Canada "FASTER" Artificial Intelligence (AI) Principles:

1. **Fair**: ensure that content from these tools does not include or amplify biases and that it complies with human rights, accessibility, and procedural and substantive fairness obligations; engage with affected stakeholders before deployment
2. **Accountable:** take responsibility for the content generated by these tools and the impacts of their use. This includes making sure generated content is accurate, legal, ethical, and compliant with the terms of use; establish monitoring and oversight mechanisms
3. **Secure:** ensure that the infrastructure and tools are appropriate for the security classification of the information and that privacy and personal information are protected; assess and manage cyber security risks and robustness when deploying a system
4. **Transparent:** identify content that has been produced using generative AI; notify users that they are interacting with an AI tool; provide information on institutional policies, appropriate use, training data and the model when deploying these tools; document decisions and be able to provide

explanations if tools are used to support decision-making
5. **Educated:** learn about the strengths, limitations and responsible use of the tools; learn how to create effective prompts and to identify potential weaknesses in the outputs
6. **Relevant:** make sure the use of generative AI tools supports user and organizational needs and contributes to better outcomes for clients; consider the environmental impacts when choosing to use a tool; identify appropriate tools for the task; AI tools aren't the best choice in every situation

Artificial Intelligence (AI) Administrative Data Safety Guidelines:

1. Google's Gemini App provides an institutionally-approved, free and secure tool to respond to the demand for access to generative AI as a productivity tool. Interactions with the Gemini App stay within the Google Workspace Cloud isolated to the College and are not reviewed by humans or otherwise used to improve Google's generative AI models.
2. The Gemini App is currently the only generative AI platform that has been endorsed for use with Olds College administrative data. While it is recommended as a safe generative AI option, in terms of data privacy and security, there are still limitations on what data is safe to use.
3. While Gemini is the endorsed College AI tool, from a data security perspective, other AI tools may be utilized under certain circumstances; however these should be approached with caution.The table below provides more details on what types of data are safe to use with Gemini or alternative AI tools.

AI Application Risk Matrix		
	Institutionally Endorsed Tool (Gemini)	**Other AI Tools**
Restricted Data	High risk	High risk
Confidential Data	Not advised	High risk
Protected Data	Endorsed	Not advised
Public Data	Endorsed	Endorsed

Legend

1. Endorsed: This type of data is generally safe to use with AI tools.
2. Not Advised: Some risks may exist, review the tool's privacy settings and terms before sharing data. Before proceeding, ensure appropriateness of data use with the data steward or data owner, in alignment with the College policies.
3. High Risk:This type of data must not be shared with the AI tool.

Digital Data Organization, Sharing & Storage Guidelines:
The following data guidelines specify best practices on how digital data is to be organized, shared and stored at the College. In alignment with B09 - Records Management and Disposition; and the B09: Records Retention & Disposition Schedule.

OLDS COLLEGE
OF AGRICULTURE & TECHNOLOGY

Organization:

1. Avoid storing the same data in multiple places to avoid duplication and ensure consistency.
2. Create a clear, logical folder hierarchy and use consistent file naming conventions to make documents easy to find.
3. Restrict access to documents based on user roles to prevent unauthorized viewing or modification.
4. Enable audit trails to track who accesses or modifies documents and when.
5. Workplace documentation should be stored on a Shared Google Drive, rather than a personal Google Drive to ensure succession and longevity.
    a. Shared drives should be utilized as much as possible to support business continuity and minimize the potential for data loss.

Security & Storage:

1. Institutional data must be stored in such a way as to ensure that the data is secure, and that access is limited to authorized users based on their roles.
    a. Secure storage of institutional data is a joint responsibility of Data Stewards and their respective Departments.
    b. IT will manage data backup and recovery, with at least one backup stored offsite or in the cloud.
2. Institutional data should not be utilized and stored on personal devices, but should instead be utilized on College technology to maintain data security and effective backup.
3. Use applicable explicit sharing settings when sharing documents and links, rather than making all documents accessible to all internal and external users, or to anyone with the link.
4. When electronic data is no longer required for administrative, legal or historical reasons, data users are responsible to dispose of the data in accordance with the Olds College Records Retention & Disposition Schedule.
5. Data Stewards and Data Users need to be clear with those providing data, about how data is going to be utilized, in alignment with provincial legislation and associated College policies.

Workflow:

1. Recommend using collaborative systems that track revision history to prevent confusion and ensure everyone is working on the most current document.
2. Create and use standard templates for recurring document types, such as invoices or reports.
3. Leverage existing College workflow systems to automate processes like document approval tracking.
4. Data Stewards need to discuss digital document retention in Departments to ensure employees understand the document management practices of the Department and associated College policies to ensure institutional and legislative compliance.

Definitions:

Administrative Data: Facts, statistics or information collected directly or indirectly by Olds College for the purpose of administrative functions; including information the College collects directly or indirectly, and any information relevant to the operations, planning or management of any unit within Olds College.

	Major Data Environment: Data within a core environment of the College; these include financial, academic and human resources areas. And are typically dominated by a core technology system (e.g. Banner for academic data). **Information Technology System:** A collection of interconnected software, hardware, people, and processes that manage information. **Data Dictionary:** A set of information describing the contents, format, and structure of data and the relationship between its elements, used to control access to and manipulation of the data. **Artificial Intelligence (AI)**: Information technology that performs tasks that would ordinarily require biological brainpower to accomplish, such as making sense of spoken language, learning behaviours or solving problems. Note, generative AI is a type of AI that produces content such as text, audio, code, videos and images. This content is produced based on information the user inputs, called a "prompt," which is typically a short instructional text (e.g. ChatGPT).
Related Information:	B01 Code of Conduct B04 Information Access & Protection of Privacy Policy B09 Records Management & Disposition Policy B09 Records Retention & Disposition Procedure C04 IT Governance & Technology Management Policy C04 IT Governance & Technology Management Procedure C04 Institutional Data Governance Procedure C04 Digital Security Procedure Data Classification Standard
Review Period:	1 year
Revision History:	New: December 2025