

Data Governance Framework

PURPOSE

This document describes the data governance framework for the University of Saskatchewan (USask). It identifies designated roles within the university that have specific decision-making accountabilities regarding university data, as well as defines the roles and accountabilities for data stewardship and data management. This framework exists to support the university's Data Management Policy.

This framework establishes a well-aligned data governance structure by delineating roles, aligning data stewardship accountabilities with the university organizational structure, and facilitating holistic and inclusive data management decision-making. This is achieved through adoption of data governance industry standards in areas such as data classification, data quality dimensions, and data access.

DATA STEWARDSHIP STRUCTURE

The USask data governance framework establishes seven roles within the data stewardship organizational structure. These seven roles each have different roles and responsibilities for decision-making regarding university data. The seven roles are:

1. Data Trustees – Highest-ranking individuals accountable for what happens with and to university (e.g. institutional, research, Indigenous, etc.) data.
2. Data Stewards – Individuals who are responsible for promoting appropriate data use through planning, policy, and protocols at the university.
3. Data Managers – Individuals responsible for ensuring that policies are followed within a specific area and that local processes are consistent with university policies and procedures.
4. Data Producers – Individuals responsible for creating or collecting university data.
5. Data Consumers – Individuals who access and use university data.
6. Data Administrators – Individuals in IT who have operational level responsibility for data management activities related to the creation, storage, maintenance, cataloguing, use, dissemination, integration, security, and disposal of data.
7. Data Specialists – Individuals who interpret and understand needs of various institutional units for data and supply those needs in custom-requested formats.

The relationship between these roles and their responsibilities as applicable at the university are described in more detail in the following section. Appendix A includes a list of university Data Trustees, while appendix B provides data management-related definitions, and Appendix C provides links to data governance reference material.

ROLES AND RESPONSIBILITIES

Data Trustees

Data trustees provide collaborative leadership, strategic direction, and accountability for what happens with and to data.

As a group, the data trustees are responsible for:

- Actively participating in the Data Governance Leadership Committee.
- Approving data management policies, guidelines, standards, and procedures.
- Approving changes to the scope of functional areas.
- Resolving issues of procedure.

As individuals, data trustees are responsible for appointing data stewards, delegating data stewardship accountabilities in their functional or research area, and establishing data stewardship committees as appropriate.

The **President** is the institutional data trustee and is the university's authority for university data and information. The institutional data trustee is responsible for:

- Ensuring that the university has a data management policy that safeguards and protects the university's data.
- Making decisions about university data in strategic and high-impact situations that could affect the entire university. These could include data decisions that involve legal precedent, involve ransom of university data, or involve disclosure of information that significantly impacts the reputation of the university.

The **Vice-President Finance and Resources** is the designated Head for the purposes of section 2(e) of The Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP). The Head has authority for all decisions made on behalf of the university pursuant to this policy and under the Act. The Vice-President Finance and Resources also oversees the Management of University Records policy.

The **Provost** is the institutional authority for decisions on the management and use of the university's data pertaining to institutional-level planning, resource allocation, budget frameworks, and the university's academic programs and academic policy.

The **Vice-Presidents, Vice-Provosts, the CIO, Associate Provosts and Associate Vice-Presidents** with senior leadership responsibilities for functional areas are data trustees for their data domain areas.

The **Principal Investigator (PI)** is the data trustee for their research and is accountable for all decisions regarding that data and for meeting the responsibilities outlined in the Responsible Conduct of Research Policy and as required by the funding agency.

Data Stewards

Senior university officials (typically at the level of directors, deans, and Principal Investigators or their delegate(s)) in university units who are responsible for promoting appropriate use of data through planning, policy, and protocols at the university.

Collective Decision-Making Responsibilities

Data stewards have stewardship responsibilities for particular elements and/or aspects of institutional data. However, in many cases data stewardship responsibilities for a particular data element span multiple functional areas resulting in shared interests among many stakeholders. For example, data about faculty has stakeholders in the Human Resources administrative unit, as well as in a dean's office; student data becomes alumni data when a student graduates; and Indigenous data crosses all functional areas.

In the situations when data is shared across multiple functions, the data stewards are responsible for:

- Following university governance practices to get proper engagement in decision making.
- Including representatives from all functional areas and communities in decisions about overlapping data sets.
- Managing collectively the data stewardship responsibilities for data that spans multiple functional areas and/or units.
- Resolving issues for data elements that span multiple functional areas and/or units. If there are any data issues that cannot be resolved at the Data Steward level, these should be escalated to the Data Trustee level.

As a group, the data stewards have a responsibility to promote and encourage a university view of the data resource, to give consideration to all stakeholders for that data, to follow university governance practise to engage with affected communities and populations groups when decisions are being made, and to ensure that its use is in line with university policies and any relevant data sharing agreements.

Individual Responsibilities

As individuals, the data stewards have specific responsibilities and authority for the management, access, use, definition, and quality of data that pertains to their functional areas and/or is deemed to be under their purview.

These responsibilities include:

- Appointing data managers and delegating operational stewardship accountabilities.
- Providing governance oversight for data within their area of responsibility, including:
 - Defining the scope of data domains and approving changes.
 - Reviewing and approving data definitions, compliance, and access classifications (public, internal, limited, and restricted).
 - Reviewing quality metrics and assessment of progress toward improvements in data integrity.
 - Prioritizing data issues for resolution.
- Approving the use of institutional data for which they are responsible, for the purposes of research.
- Approving and ensuring compliance regarding the release of, responsible use of, and access to data for which they are responsible.
- Approving the appropriate access of data by vendors and agents, while ensuring that agreements about the use and disclosure of such data are negotiated, documented, and compliant with regulatory requirements and university policies.
- Recognizing when data belongs to and/or affects a particular community (e.g. Indigenous communities) or segment of the population (e.g. gender identity), or relates to dimensions or attributes within such groups, and then:
 - Seeking out either the established groups or dedicated individuals at the university that specialize in engagement with that community or segment of the population.
- Actively participating in the Data Stewardship Committees.

In the case of research data, the PI (or delegate) is the data steward for the data associated with their research and is responsible for all decisions regarding that data. The PI (or delegate) is also responsible for meeting the responsibilities outlined in the Responsible Conduct of Research Policy and as required by their funding agencies.

Data Managers

Data managers are individuals in positions with operational responsibility for institutional data. They are responsible for ensuring that policies are followed within a specific area and that local processes are consistent with university policies and procedures.

Both as individuals and collectively, responsibilities of data managers for institutional data include:

- Developing data definitions.
- Assessing and documenting data compliance.
- Categorizing data into access classifications (public, internal, limited, and restricted).
- Reviewing and approving requests for data access, if delegated to them.
- Assessing data quality.
- Identifying and documenting data issues and ensuring the issues are addressed.
- Identifying source systems of record.
- Working collaboratively with other functional areas and following university governance practices for data management.
- Recognizing when data belongs to and/or affects a particular community (e.g. Indigenous communities) or segment of the population (e.g. gender identity), or relates to dimensions or attributes within such groups, and then:
 - Seeking out either the established groups or dedicated individuals at the university that specialize in engagement with that community or segment of the population.

In the case of research data, the PI (or delegate) is the data manager and is responsible for meeting the data management responsibilities outlined in the Responsible Conduct of Research Policy and as required by the funding agencies.

Data Producers

Data producers are employees of the university who collect, create, update, or delete data during the regular course of their day-to-day activities. Every employee has the potential to be a data producer either through their job responsibilities (e.g. creating class build data, entering new employee data) or through their role as an employee (e.g. submitting expense claims and time reporting).

Responsibilities of data producers for institutional data include:

- Creating, collecting, and updating university data in a way that maintains good data quality (i.e. accurate, consistent, and timely).
- Contacting the appropriate data manager/resource person when there are questions on how data should be collected, created, or updated.
- Complying with university retention and disposition schedules and other procedures related to the management of university records.

If data producers intend to collect data outside of approved university systems, they are responsible for:

- Finding out if the data is already available in a university system.
- Verifying that the data is being collected for an appropriate purpose.
- Assessing if collecting the data complies with privacy legislation.
- Contacting the appropriate data manager/data steward or privacy officer for assistance.

In the case of research data, the PI (or delegate) is the data producer and is responsible for meeting the data management responsibilities outlined in the Responsible Conduct of Research Policy and as required by the funding agencies.

Data Consumers

Data consumers are individuals at the university who have been granted access to university data in order to carry out their assigned duties or in fulfillment of their role at the University of Saskatchewan. In some cases, this includes individuals who are external to the university, such as auditors or researchers from a different institution.

Data consumers are responsible for:

- Complying with the institutional data policies and following established procedures, such as data storage and handling guidelines.
- Understanding the definition, quality, and usage limitations of data.
- Protecting the data within their care in any format (e.g. print, digital).
- Protecting their data access privileges from unauthorized use.

Data Specialists

Data specialists are individuals at the university who interpret and understand the needs of various university units for data and provide data-driven information to meet those needs.

Their data management responsibilities may include:

- Analyzing data to support the identification of emerging trends, development of metrics and comparators, etc.
- Providing definitions, compliance, and access recommendations for data.
- Developing data profiles to facilitate data quality assessments.
- Facilitating data governance working groups and committees.
- Providing training and facilitation on data governance.
- Facilitating and supporting the threat and risk assessment/privacy impact assessment (TRA/PIA) process.

In the case of research data, the PI (or delegate) is the data specialist and is responsible for meeting the data management responsibilities outlined in the Responsible Conduct of Research Policy and as required by the funding agencies.

Data Administrators

Data administrators are ICT personnel who have operational level responsibility for data management activities related to the creation, storage, maintenance, cataloguing, use, dissemination, and disposal of data.

Their data management responsibilities may include:

- Providing access to secure facilities and services to support data management activities.
- Implementing access and security controls based on access classifications.
- Developing QA processes to identify data issues.
- Maintaining the underlying data infrastructure and an easy-to-use, accessible data dictionary.
- Facilitating and supporting the threat and risk assessment/privacy impact assessment (TRA/PIA) process.

In the case of research data, the PI (or delegate(s)) is responsible to work with data administrators in ICT in order to meet their data management responsibilities to protect and secure their research data as outlined in the Responsible Conduct of Research Policy and as required by the funding agencies.

INSTITUTIONAL DATA GOVERNANCE STRUCTURES

In order to support the institutional data governance activities of the university, three types of governance bodies exist. Committees and working groups are organized around functional areas and data domains. They include:

- Data Governance Leadership Committee – Members include the Data Trustees.

- Data Stewardship Committees – Members include Data Stewards.
- Data Working Groups – Members include Data Managers, Data Specialists, and Data Administrators.

These committees and working groups generally meet on a regular basis to address data issues appropriate for their level of responsibility.

RESEARCH DATA GOVERNANCE STRUCTURES

Principal Investigators (PI), in their role as Data Trustees for research data, are accountable for what happens with and to their research data. Given the variation in the scale and jurisdiction of different research projects, the PI may also act as data steward and data manager for their research data, or choose to delegate those responsibilities to others involved in their research.

Additional data governance structures include:

- Research ethics boards
- Funding agencies (e.g. Tri-Agency)
- Partner entities

Appendix A – List of University of Saskatchewan Data Trustees

Data trustees have stewardship accountability for all data; however, each data trustee has areas of data responsibility for which they have expertise, and these areas may overlap each other. For example, data about Indigenous faculty would cross the areas of data responsibility for Vice-Provost, Indigenous Engagement, Vice-Provost Faculty Relations, and Associate Vice-President People & Resources.

Trustee Position	Trustee Name	Areas of Data Responsibility
President	Peter Stoicheff	University data
Vice-President, Administration	Greg Fowler	Freedom of information and protection of privacy matters and Records Management Financial data
Provost	Airini	Data pertaining to institutional-level planning and the university's academic programs and academic policy
Vice-Provost, Indigenous Engagement	Angela Jaime	Data created or collected by the university that is associated with Indigenous individuals or Indigenous communities Data created, collected, or derived from research, scholarly, and artistic activity associated with Indigenous individuals or Indigenous communities
Vice-Provost, Students and Learning	Jerome Cranston	Student and student services data Administrative data about teaching and learning activities Health and wellness data
Principal Investigator	Various	Data created or derived from research, scholarly, and artistic activity
Associate Vice-President(s), Research	Terry Fonstad	Administrative data about research activities
Vice-Provost, Faculty Relations	Scott Walsworth	Data about faculty, including data contained in Curriculum Vitae
Associate Vice-President, People and Chief Human Resources Officer	Marnie Wright	Human resources data
Chief Financial Officer	Deidre Henne	Data pertaining to resource allocation and budget frameworks
Associate Vice-President, Services	Wade Epp	Data about the university's operational services and physical assets
Vice-President, University Relations	Cheryl Hamelin	Alumni, donor relations, and communications data
Dean, University Library	Charlene Sorensen (Interim)	Data about library collections and circulation
Associate Vice-President, Information and Communication Technology and Chief Information Officer	Michael Barr	Data pertaining to central identity services that are shared across all functional areas

Appendix B – Definitions

- **Academic home** –The college, school, division, department or unit in which the Principal Investigator holds their primary appointment.
- **Administering unit** – The college, school, division, department, centre or other university unit that accepts administrative responsibility for a Funded or Non-Funded Research Project. In cases where the Administering Unit is not the Academic Home of the Principal Investigator, they may transfer administrative responsibility for a Funded or Non-Funded Research Project to an Administering Unit with approval from their Academic Home and the Administering Unit that accepts the administrative responsibility.
- **Data classification** – The act of grouping data into categories that are used to facilitate access to institutional data. The categories balance the sensitivity of the data with business need to access the data, while taking into consideration the impact of unintended disclosure of the data.
- **Data domain** – A sub-grouping of data within a functional area or a research project.
- **Data governance** – Establishing and maintaining the processes by which decisions regarding data are made. It includes establishing the data governance framework, approving data processes and resolving disputes concerning data issues.
- **Data management** – Encompasses activities that relate to the creation, collection, storage, maintenance, cataloguing, use, dissemination and disposal of university data.
- **Data stewardship** – Ensuring that institutional data are reliable, consistent and of high quality and that they are accessible for appropriate purposes, people and systems; ensuring that institutional management practices comply with government legislation (e.g. PIPEDA, HIPA) and industry standards (e.g. Payment Card Industry Data Security Standard).
- **Derived data** – Data that is transformed from other data using a mechanism such as an arithmetic formula, composition, or aggregation.
- **Functional areas** – A broad category of data that groups data based on type and use, such as student, employee, and advancement. These can be further divided into data domains. In the case of research data, the functional area is the research project.
- **Principal Investigator (PI)** – The individual responsible for the intellectual leadership of a Research Project or Research Program. For clinical Research, the PI is defined as the person responsible for the conduct of clinical Research at a Research site, which is where the clinical trial related activities are conducted.
- **University community** – All students, employees, faculty, postdoctoral fellows, researchers, alumni, agents, contractors, authorized guests, persons or organizations acting for or on behalf of the university.

- **University data** – Data that is created, collected and stored (either electronically or in hard copy) by units and members of the university community, in support of academic, research, and administrative activities.

University data may include the following (these are not mutually exclusive):

- **Institutional data** – Data that is created, collected, and stored by all units and members of the university community, in support of academic and administrative activities. Data about research, scholarly and artistic activity, such as research grants held and publications generated, is considered institutional data.
- **Research data** – Data that is created by or derived from research, scholarly, and artistic activities.
- **Personal data** – Data that contains personal information about an identifiable individual as defined in the Provincial Local Authority Freedom of Information and Protection of Privacy Act (LAFOIPP). This data, if compromised or used inappropriately, would have implications to the privacy of an individual.
- **Indigenous data** – Data created or collected by the university that is associated with Indigenous individuals or communities.
- **Indigenous research data** – Data created or derived from research, scholarly, and artistic activity associated with Indigenous communities.
- **Third-party data** – Data that is created or owned by a third party and is being used in support of academic, research and administrative activities. This data if compromised or used inappropriately would have implications for the third party. This includes data such as licensed software or software components, and copyrighted material.

Appendix C – Data Governance Reference Material

University of Saskatchewan Data-related Policies

- [Data Management Policy](#)
- [Responsible Conduct of Research Policy](#)
- [Information Technology Use](#)
- [Information Technology Security Policy](#)
- [Management of University Records Policy](#)
- [Freedom of Information and Protection of Privacy Policy](#)

University of Saskatchewan Data Management Resources

- [Data Classifications](#)
- [Data Storage and Handling Guidelines](#)
- [Enterprise Architecture Principles](#)
- [Research Data Management Strategy](#)

External Data Management Resources

- [The First Nations Principles of OCAP \(Ownership, Control, Access, and Possession\)](#)
- [United Nations Declaration on the Rights of Indigenous Peoples](#)
- [CARE Principles for Indigenous Data Governance](#)
- [FAIR Guiding Principles for Scientific Data Management and Stewardship \(Findable, Accessible, Interoperable, and Reusable\)](#)
- [COBIT IT Governance Framework](#)

Data-related Legislation

- [Provincial Local Authority Freedom of Information and Protection of Privacy Act \(LAFOIPP\)](#)
- [Federal Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#)
- [Health Information Protection Act \(HIPA\)](#)