Data Ethics Framework

Innovation, Privacy and Policy Division and Data and Content Management Division, Technology and Innovation

Version: 1.0

Approved by: ADM, Innovation, Privacy and Policy Division	**Owner:** Innovation, Privacy and Policy Division	
Approval date: January 25, 2024	**Last Reviewed:** January 22, 2024	**Review Date:** January 22, 2026
Contact: Innovation, Privacy and Policy Division	**Policy Instrument type:** Framework	

Contents

Introduction and Purpose

The Government of Alberta (GoA) is accountable for, and committed to the ethical creation, collection, management (including access, disclosure, disposition) and use of data.

This framework provides high-level strategic direction to maintain consistent and effective data ethics across the GoA in the rapidly evolving digital world. The Data Ethics Framework (DEF) demonstrates the GoA's commitment to data ethics by:

- specifying principles that will inform the development of new and/or revision of existing policy instruments; and
- highlighting data ethics-related commitments the GoA will implement in support of the framework principles.

All GoA staff manage and use data. Decisions and actions involving data are context-dependent and evolve over time. For this reason, assessing data ethics is an ongoing process. The DEF supports data governance by incorporating ethical principles in decision-making about data to maintain public trust and deliver programs and services for the benefit of Albertans.

The framework must be interpreted in the context of all applicable legislation, including the *Freedom of Information and Protection of Privacy Act* (FOIP), *Health Information Act* (HIA), and/or legislation specific to any department's governance and operations. Legislation is paramount to any internal GoA policy instrument.

Executives and staff must also apply this framework in the context of:

- the Oath of Office;
- Alberta Public Service Vision and Values;
- the Code of Conduct and Ethics for the Alberta Public Service; and
- existing department policies and practices for ethical behaviour.

This framework is not intended to provide operational recommendations or implementation insight, as subsequent policy instruments will be developed in alignment with the framework principles.

NOTE: Data ethical frameworks do not replace, but rather complement, support and are interconnected with relevant hard law instruments such as regulations on privacy, data protection, open data, open government, transparency and data sharing within the public sector, among others.

- Organization for Economic Co-Operation and Development (OECD)

Development of this framework was guided by and informed by OECD's "Good Practice Principles for Data Ethics in the Public Sector", and extensive cross-government engagement.

Vision

The GoA is trusted by the public to engage in practices and behaviours that are ethical. This includes the creation, collection, management and use of data. The GoA understands the ethical implications connected to all data, which it uses to develop, deliver and maintain programs, services and policy.

Framework Scope

The principles identified in the framework are relevant to anyone working directly or indirectly with data in Alberta's public sector, including data practitioners (statisticians, analysts, and data scientists), operational staff, those developing data-informed recommendations and policy, and decision-makers.

There are ethical considerations for the use of all data, not just personally identifying information or information of a sensitive or confidential nature.

Benefits

A government-wide framework for data ethics will:

- establish consistent principles to guide government decision-making around the creation, collection, management, and use of data;
- enhance understanding of the risks and limitations inherent in the use of data for analysis and decision-making (such as biased data, arguments based on an absence of evidence, and misapplication of statistical concepts);
- ensure data collection considers the diversity and perspectives of individuals that the data pertains to and that data collectors are aware that some historical data collected has resulted in discriminatory activities and breaches of trust with marginalized or equity-seeking individuals and groups; and
- strengthen Albertans' confidence that government will use data fairly and transparently in the public interest.

Framework Principles

Considering ethics when working with data helps mitigate risk to Albertans, the GoA, and the wider public. This framework is organized around four core principles:

- **Accountability**: Oversight, control and education are maintained to ensure that employees are collecting, managing and using data ethically to support programs and services.
- **Equity**: Unintended discriminatory effects on individuals and groups are reduced within data or derived products and services.
- **Privacy and Protection**: Privacy and protection are maintained through a "privacy by design" approach, ensuring that only data that is required is collected, managed and accessed appropriately, and used in a manner that respects the individuals' rights to privacy.
- **Transparency**: Intent for the use of data is clearly communicated to individuals and organizations, including how the data will inform the development and operation of GoA services and programs.

These principles must inform decision-making about data use and must be considered at all stages of the Information Management Lifecycle; create/collect, organize, use/access, disposition, store/manage, and protect.

Accountability

The GoA maintains oversight, control and education to ensure that employees are collecting, managing and using data ethically to support programs and services. Demonstrating accountability enhances trust, data quality, and the responsible creation, collection, management, and use of data. In the GoA, accountability flows from the Crown to ministers, then to deputy heads (or equivalent).

The deputy head of a department is ultimately accountable for the data in the custody and/or under the control of their department. When accountability for data resides with more than one department, governance is established in enterprise and department policy instruments.

The GoA will:

- manage risks and minimize potential for negative consequences through effective enterprise governance and processes;
- use effective governance and oversight mechanisms for the creation, collection (including acquisition,) management, and use of data and data sets;
- prioritize reliable data assets by ensuring:
  - data created or collected conforms to data standards.
  - data is recorded accurately, attempts are made to resolve data errors, and unresolved errors are documented.
  - data lineage is documented, including why the data was collected and any conditions and restrictions. The data lineage includes how and why data changes occurred.
- apply security models and controls and conduct security audits on a regular basis;
- document department data governance structures, including Data Executives and Data Stewards as specified in the Data Management Roles Directive;
- ensure data management policies are correctly applied; and
- ensure data assets are managed appropriately in accordance with applicable policy instruments.

Support Mechanisms

The policy instruments and processes that support accountability include (but are not limited to):

- Content Management Policy;
- Information Controller and Information Custodian Directive and Guideline; and
- Data Management Roles Directive.

Equity

The GoA will reduce unintended discriminatory effects on individuals and groups within data or derived products and services. Enhancing equity leads to the development and delivery of fair and effective programs and services.

Decision-makers must understand both the limitations of the data and any potential biases inherent in the data and how it was collected. To mitigate potential harm, the risks associated with biases both in the data itself and the decisions made with that data need to be thoroughly understood.

The GoA will:

- consider the views of the public on the data used and the perceived benefits of that use;

- reflect interests of Indigenous Peoples and other marginalized groups when measuring, collecting and reporting data relating to those populations;
- recognize the equal value of knowledge shared by Indigenous Peoples and carefully consider the need for respectful, appropriate access to, use, and protection of this knowledge;
- identify and mitigate assumptions and sources of bias within data;
- provide thorough explanations for collecting sensitive data (including race, gender, ethnicity, etc.) from historically marginalized individuals and groups to proactively address potential concerns of discriminatory activities and biased decisions;
- not use data to harm any individual, organization, or group;
- implement strategies to minimize harm and reduce bias; and
- remove biases where possible; use data for stated and documented purpose; actively assess data for unintentional bias.

Support Mechanisms
The policy instruments and processes that support equity include (but are not limited to):

- Various policy instruments are in development or will be developed to support this principle.
- Administrative Fairness Guidelines | Alberta Ombudsman

Privacy and Protection

The GoA will implement a "privacy by design[1]" approach, ensuring that only data that is required is collected, managed, and accessed appropriately, and used in a manner that respects the individuals' rights to privacy. Enhancing privacy and protection leads to the delivery of services that are secure, safe to use and trusted.

An important aspect of complying with privacy legislation is demonstrating what measures are taken to ensure privacy is protected. The GoA has the legislated responsibility to protect personal information in its custody and/or under its control and ensure privacy is maintained at the highest level via policy, control mechanisms, and staff training.

The GoA will:

- respect the privacy and confidentiality of individuals and institutions;
- elevate the importance of privacy when developing and/or leveraging innovative, emerging technologies;
- have processes to accept data subject's requests for access to data about themselves and to seek correction in data sets or collections;
- evaluate benefits of enabling individuals to seek removal from data sets or collections;
- evaluate benefits and risks of severing personally identifiable information from data and retaining the anonymized data for continued analysis;
- prevent unauthorized access, collection, use, disclosure and/or destruction of personal information; and
- keep data confidential and secure with appropriate access controls and audits.

[1] Privacy by design goes beyond the scope of this framework and is addressed in more detail in the Privacy Management Framework. It is essential for Department Data Executives and Data Stewards to understand and demonstrate how privacy concerns are addressed throughout the information management lifecycle for a particular data asset.

Support Mechanisms
The policy instruments and processes that support privacy and protection include (but are not limited to):

- *Freedom of Information and Protection of Privacy Act*;
- Privacy Management Framework
- Privacy Breach Procedure (no external access)
- Cybersecurity Policy (no external access)
- Cybersecurity Control Framework (no external access)
- Information Security Management Directives
- Security Incident Response Process (no external access)
- Acceptable Use of Third-Party Natural Language Generators Directive and Guideline
- Data and Information Security Classification Standard and Guideline
- Data and Information Security on Premise Standard (no external access)
- Data and Information Security in the Cloud Standard (no external access)
- Secure Digital Media Sanitization Standard (no external access)
- Cryptographic Algorithms Standard (no external access)

Transparency

The GoA will clearly communicate its intent for the use of data with individuals and organizations, including how the data will inform the development and operation of GoA services and programs. Enhancing transparency leads to easy-to-understand communication about government principles, policies, and processes for data.

Transparency around the creation, collection, management, and use of data fosters a culture of trust between government and individuals and organizations.

The GoA will:

- document processes, lineage and methodologies for data assets and where appropriate make the methodologies for processing the data available in an easily accessible format;
    - Documented methodologies should include any data transformations and data quality issues, as well as metadata, data lineage (including context of data use), data glossaries, and consent and usage notifications.
    - Where possible, bias in each phase of the data lifecycle is clearly articulated and understood by all data users, and mitigation plans enacted.
- communicate open data principles to stakeholders;
- publicly release government owned data, if appropriate and not subject to privacy, security, or legislative restrictions; and
- compose collection notifications with enough detail that those providing the data (for example, data subjects, organizations, etc.) can understand the breadth and variety of data that will be collected, the lifecycle of the data asset, potential uses, and any possible benefits and harms associated with collection and use of the data.
    - A linked data disclaimer that anticipates how data will be used in the future should be developed by the data collector. The disclaimer must be clearly communicated to individuals and organizations.

Note: Any disclosure of data must follow existing legislation and policies.

Support Mechanisms
The policy instruments and processes that support transparency include (but are not limited to):

- Open Information and Open Data Policy; and
- Developing a FOIP Collection Notice Standard.

Contact

For any questions regarding the Data Ethics Framework please contact Technology and Innovation’s Innovation, Privacy and Policy Division.

Appendix A – Definitions

Content encompasses all the records, data and/or information, regardless of format, state and/or classification (for example, official, transitory, active, semi-active, inactive, open, closed, etc.) that are part of, or are affected by, a business area's processes.

(Source: Data Management Roles Directive)

Data refers to facts represented as text, numbers, graphics, images, sounds or video. Data is the raw material required to assemble information or from which information can be derived. Data becomes information by interpretation.

(Source: DAMA Dictionary of Data Management)

Record: a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded, or stored in any manner, but does not include software or any mechanism that produces records.

(Source: *Freedom of Information and Protection of Privacy Act*)

The GoA Content Management Policy includes additional definitions of key content management concepts that can support a common understanding of the framework.