Data Ethics Framework Toolkit

Introduction

> Technology and Innovation is dedicated to assisting departments, agencies, boards, and commissions in applying the Data Ethics Framework (DEF) when initiating a new program, service, and/or application.

The DEF Toolkit is intended to help staff understand the application of its four guiding principles (**Accountability**, **Equity**, **Privacy and Protection**, and **Transparency)**. The toolkit is available to all Alberta Public Service employees and is intended to be used in combination with the DEF.

Overview of the Data Ethics Framework

The DEF provides high-level strategic direction to maintain consistent and effective data ethics across the Government of Alberta (GoA) in the rapidly evolving digital world.

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 Principles

Accountability

Oversight, control, and education are maintained to ensure that employees are collecting, managing, and using data ethically to support programs and services.

Applying the Principle

- Complete all mandatory training with the intent to meaningfully apply it and ensure awareness and familiarity with policy instruments for data management, as they are frequently reviewed/enhanced/created to ensure relevance; mandatory training is identified in the Learning section of 1GX and includes topics such as FOIP/Privacy, Information/Data Management, and Cybersecurity (enterprise policy instruments on these topics can be found on the Information Management and Technology Policy Instruments site and are referenced in the DEF).
- Ensure awareness of key data roles that have been designated in your area and engage them appropriately for data-related matters (for example, Data Executives and Data Stewards).
- Frequently review documentation about data assets to ensure reliability, which includes:
  - validation that data conforms to established data standards;
  - confirmation that the data has been captured accurately, and attempts have been made to resolve errors (unresolved errors are to be documented); and
  - understanding data lineage (for example, why the data was collected, changes to the data, and any conditions/restrictions on its use).
- Become familiar with the systems that hold or manage data to ensure any potential issues (for example, system verification of data accuracy or inconsistencies) are flagged and brought to the attention of leadership, and the appropriate access restrictions are in place to prevent unauthorized access.

Equity

Unintended discriminatory effects on individuals and groups are reduced within data or derived products and services.

Applying the Principle

- When collecting personal data, consult with the Privacy Services team in Technology and Innovation to develop clear and detailed Freedom of Information and Protection of Privacy collection notices that meet legislative requirements.
- Frequently review (and re-design if necessary) the program and existing data collection methodologies to ensure:
  - data is not being used to harm any individual, organization, or group, and mitigation strategies are in place;
  - data collection adheres to legislated requirements (for example, only necessary data is collected); and
  - existing data is not compromised by known and/or unconscious bias (recollect if necessary).

- Ensure consideration is given to how the public will perceive data collection or data use, and provide easily accessible mechanisms for their feedback.
- Ensure interests of Indigenous Peoples and other marginalized and diverse groups are incorporated when measuring, collecting, and reporting data relating to those populations.
  - Include Indigenous Peoples and marginalized and diverse groups in focus groups to ensure impacts of use of data relating to these populations are accurately captured and understood (avoid assumptions).
  - Become familiar with and respect Indigenous data sovereignty, and ensure Indigenous Peoples are consulted before collecting or using data about them.

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.

Applying the Principle

- Become familiar with the Privacy Management Framework and consult with the Privacy Services team for advice regarding authority to collect, use, and disclose personal information.
- Complete all mandatory training and become familiar with and adhere to enterprise policies and guidance; mandatory training is identified in the Learning section of 1GX and includes topics such as FOIP/Privacy, Information Management, and Cybersecurity (enterprise policy instruments on these topics can be found on the Information Management and Technology Policy Instruments site and are and are listed on the DEF page).
- When developing or implementing new technologies or programs, ensure privacy considerations are incorporated into all stages of program and service design, development, and implementation. This means engaging with the necessary parties (such as Privacy Services, Cybersecurity, etc.) early in program development.
- Familiarize yourself with and routinely implement practices to safeguard data, such as:
  - practicing a clean desk policy, including when working remotely;
  - not distributing government data through personal email;
  - locking your computer when away from your desk; and
  - using locked bins for the secure destruction of transitory documents.
- As new standards and processes are developed, adhere to data standards, processes, and methodologies to ensure data anonymization requirements are adhered to and complete; alternative data sources may also need to be considered (for example, synthetic data) to ensure the protection of personal information.
- Become familiar with and adhere to requirements for requests made by an individual to have their personal data updated and/or removed from GoA systems.

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.

Applying the Principle

- Develop and frequently review documentation (processes, data lineage, methodologies) to ensure the use of plain language to enhance understanding within the GoA and for the public.
  - Identify opportunities to publish, where appropriate, on program websites in easily accessible formats.
- Become familiar and promote open data principles within your team and with stakeholders, and, in accordance with internal process and legislative requirements, seek to publish data sets on the Open Government Portal.
- When collecting personal information for programs and services, consult with the Privacy Services team to develop clear and detailed Freedom of Information and Protection of Privacy collection notices that meet legislative requirements.
- Identify and promote training opportunities on how to develop/maintain accurate data-related documentation (such as methodologies) that captures data transformations, quality, bias, metadata, lineage, glossaries, usage requirements, etc.

Resources

- Additional resources and support mechanisms are provided in the DEF.

Contacts

- If you have questions about the DEF or Information Management and Technology policy instruments, contact imt.policy@gov.ab.ca