Province of British Columbia

Data Management Policy

Version 1.0.2

Apr. 17, 2024

TABLE OF CONTENTS

Purpose

The Data Management Policy (hereafter, “this Policy”) outlines high-level requirements for ministries to manage data in their custody and/or control. Data, like records, is a subset of information and this Policy expands on requirements found in law and other policies, such as the Managing Government Information Policy.

Overview

The foundation of a modern, digital government is based on ethically collected, accurate, and accessible data. Data can increase efficiency, improve service delivery, shape policy, and inform decisions to create a better British Columbia for all. To fully realize the benefits of data, it is imperative that ministries have a cohesive approach to data management.

Government is committed to reconciliation, equity, and developing an efficient public service that represents the diversity of the people who live in British Columbia. This commitment includes respecting the rights of Indigenous Peoples to self-determination to freely pursue their economic, social, and cultural development, and have their own languages, cultures, traditions, histories, and aspirations reflected in government systems and services. Ministries must consider these commitments when making decisions about data, including how it is collected, stored, shared, and used.

Government is responsible for the collection, management, and use of a significant amount of data and this Policy is one of the tools designed to help ministries manage their data consistently and ethically in a strategic and user-focused way. This Policy must be considered in conjunction with:

- Government’s Digital Policies and Standards
- Applicable legislation, including the Information Management Act (IMA) the Freedom of Information and Protection of Privacy Act (FOIPPA) and the Anti-Racism Data Act (ARDA)
- The United Nations Declaration on the Rights of Indigenous Peoples (UN Declaration) and the Declaration on the Rights of Indigenous Peoples Act
- The Core Policy and Procedures Manual, in particular, Chapter 12: Information Management and Information Technology Management
- The Managing Government Information Policy (MGIP)
- Directives and guidelines issued by the Chief Records Officer under the Information Management Act

- Government's IM/IT policies and standards, in particular, the Appropriate Use of Government Information and Information Technology Policy (PDF, 178K)
- Other corporate policies, standards and strategic directions issued by government, including the Standards of Conduct for BC Public Service Employees

The terms custody and control are used throughout this Policy and understanding how they differ matters for interpreting certain policy requirements.

Application

This Policy applies to all ministries and central agencies subject (hereafter, "ministries") to the Core Policy and Procedures Manual.

Authority

Core Policy and Procedures Manual, Chapter 12

Advice on this Policy

For questions or comments regarding this Policy or data management more broadly, please contact:

BC Data Service Division
Ministry of Citizens' Services
Data Systems and Services Client Hub

For questions or comments regarding information management more broadly, please contact:

Government Records Service, Corporate Information and Records Management Office, Office of the Chief Information Officer, Ministry of Citizens' Services
Email: GRS@gov.bc.ca

POLICY REQUIREMENTS

1 Data Governance

Data governance includes roles and responsibilities, decision-making, policies, and initiatives related to data. It is important to define responsibility for data because it is often copied, reused, or created in collaboration with multiple interested parties. Responsibility for a ministry's data governance is delegated by their Deputy Minister in accordance with Chapter 12.

1.1 Ministries must be able to identify point(s) of contact to oversee the governance of data in their custody and/or control.

2 Data Creation and Collection

Data is crucial to government meeting its objectives and making life better for people in British Columbia. Government creates and collects data to support research, planning, policy, legislation, program, and service delivery. Data also supports monitoring and evaluation activities, including compliance with FOIPPA, MGIP and privacy, and security requirements in the Information Security Policy and Guidelines and the Privacy Management & Accountability Policy (PMAP).

2.1 Ministries must, wherever practical, create and collect data using digital means (e.g., web forms) over the use of paper forms and redundant data entry.

2.2 Ministries must ensure the purpose for data creation or collection is clearly documented.

2.3 Ministries should ensure that data is not already available from a B.C. Government source (e.g., BC Data Catalogue and ministry data catalogues), or from other reliable sources before creating or collecting it.

Authoritative Data

Authoritative data is critical for government decision making and service delivery. The corporate-level data governance (e.g., the Deputy Minister Committee on Digital and Data) establishes the processes to govern authoritative data.

2.4 Ministries must follow the corporate processes for identifying and establishing authoritative data.

2.5 Ministries must maintain the authoritative data in their control.

3 Data Sharing, Access, and Use

Access to government data is foundational to a data-informed public service. This Policy encourages and enables public servants to use available data to make evidence-based decisions that improve outcomes for people in British Columbia. Data sharing makes data accessible to and/or enables the exchange of data between various organizations, peoples, and technologies.

By improving data sharing, ministries can increase the efficiency of data and improve collaboration between public bodies and organizations, leading to better decision making when evaluating and improving programs and services (e.g., Data Innovation Program). Whenever possible, ministries should make data open following the Open Information and Open Data Policy. Where Open Data is not appropriate, ministries should share data in accordance with the risks and benefits of its use.

3.1 Where authorized and practical, ministries must share the data in their custody and/or control with other ministries to support government administration and evidence-based decision making.

3.2 To maximize the value of government data, ministries should ensure data in their custody and/or control can be accessed and reused as appropriate in a way that meets the needs of other ministries.

3.3 Ministries should share data in a way that is proportionate to the sensitivity of the data, the benefits of its use, and protections in place.

Data Cataloguing

A data catalogue helps maximize sharing and re-use of data across government and beyond. The BC Data Catalogue is government's corporate data catalogue, where ministries are expected to list their data resources.

3.4 Ministries must catalogue high value data in their control in accordance with the Core Administrative and Descriptive Metadata Standard. This includes critical information and authoritative data.

3.5 Ministries must ensure their data catalogues are publicly discoverable, accessible, and useable.

4 Data Quality Assurance

Ministries are accountable for the quality of the data in their control. This includes ensuring the integrity of the data with respect to accuracy and completeness. Good data quality supports better decisions and service delivery.

4.1 Ministries must ensure the quality of the data in their control meets the purpose and needs of intended and secondary data users.

5 Data Documentation and Interoperability

Data Documentation

Data documentation (e.g., for design, definitions, descriptions, plans) help ministries understand their data holdings and data-related business needs. Data documentation also supports data sharing and can enable identification of redundant data creation or collection.

5.1 For the data in their custody and/or control, ministries must develop plans, structures, metadata, data models, and data flow diagrams to ensure the data is understood and meets current and long-term needs.

Data Interoperability

Interoperability enables different data systems to communicate and exchange data. Data that is interoperable is easier to share and use within ministries, across government, and beyond.

5.2 Ministries must enable effective data exchange between government systems, and where authorized, should support data exchange between government, broader public sector, and private enterprise.

5.3 Ministries should follow the Application Programming Interface (API) Guidelines.

6 Data Security and Privacy

Embedding security and privacy for data into all stages of its lifecycle ensures that it is managed appropriately and protected where required by Core Policy and Procedures Manual Chapter 15. Data protection processes can help ministries with data security and privacy. Ministries are also expected to follow the Privacy Management and Accountability Policy (PMAP) and Information Security Policy.

6.1 Ministries must determine the sensitivity of the data in their control and should classify it using the Information Security Classification Standard.

6.2 Ministries must identify security protections based on the sensitivity of the data in their custody and/or control.

6.3 Ministries must ensure appropriate security and privacy protections are applied to data throughout all stages of its lifecycle.

7 Evaluation and Compliance

While ministries are responsible for evaluating their own data management practices and the frequency with which this work is performed, setting a corporate-level policy foundation for evaluation and compliance facilitates and encourages ministries to strive towards the objectives of this Policy and the direction that it supports.

7.1 Ministries must regularly (e.g., every 2 years) evaluate their data management practices and assess their data management maturity and compliance with applicable legislation, policies, and standards.

ROLES AND RESPONSIBILITIES

Deputy Ministers

Deputy ministers have the responsibility to:

- Provide strategic direction concerning data in their ministry's custody and/or control to increase data discovery, access, sharing, and use
- Identify their ministry's authoritative data, and follow any corporate standards related to authoritative data
- Oversee the development and implementation of ministry-specific policies, processes, and procedures to support data management
- Promote the importance of data by advocating for and supporting data knowledge and skills development in their ministry
- Ensure that ministry-specific data management resources are in place to guide and support adherence to corporate policies, standards, processes, and procedures

- Establish and maintain data governance, typically fulfilled by delegation to senior-level point(s) of contact who will:
    - Oversee data in their ministry's custody and/or control,
    - Ensure alignment with corporate-level data governance (e.g., the Deputy Minister Committee on Digital & Data), and
    - Ensure that the ministry's data is managed in accordance with applicable legislation and corporate policies, standards, processes, and procedures

Government Chief Information Officer

The Government Chief Information Officer, or delegate, has the responsibility to:

- Provide strategic corporate direction related to government data
- Collaborate with ministries to develop clear and adequate data management policies, standards, processes, and procedures
- Provide expert advice and services to help ministries meet their data management obligations
- Promote the importance of data by advocating for data knowledge and skills for government
- Administer government's corporate data catalogue (i.e., the BC Data Catalogue)
- Develop and maintain the process for identifying, reviewing and approving authoritative government data
- Oversee the approval of authoritative government data and maintain a publicly accessible authoritative government data directory
- Administer the government's data governance model

Data Custodian

For the data assigned to them, data custodians have the responsibility to:

- Oversee the management of data throughout its lifecycle
- Ensure intended users of the data are supported and trained appropriately
- Meet the requirements of applicable laws, policies, and standards, including this Policy

DEFINITIONS

Note: Where terms are already defined in other documents, references have been provided to assist understanding of this Policy.

Accessible: The characteristic of being easily reached, retrieved, or used by people regardless of abilities. In the context of Information management, accessibility refers to the availability and usability of recorded information (MGIP, p.8).

Authoritative data: Data located in any repository system that is recognized through governance, law, or common acceptance as the source of origin for accurate data on a specific topic. Authoritative data may be stored in a data register.

Control: Control refers to having responsibility for the data during all or part of its lifecycle.

Custody: Custody means to have a copy of data, which may include having control over it.

Data: The smallest meaningful units of recorded information generated by an organization, which gain significance when stored in a structured manner that enables them to be synthesized and interpreted (MGIP, p.9).

Data catalogue: A data catalogue is a listing of data in an organization (e.g., BC Data Catalogue) that is designed to help data users quickly find appropriate data for any analytical or business purpose.

Data documentation: The process of recording the contextual information needed to discover, understand, interpret, use, and manage the data. This can include documentation related to data design, sampling, definition, collection, modelling, cleansing, and analysis. Data documentation is not a one-time requirement or retrospective task, but rather an active and ongoing process throughout the course of the data lifecycle. Metadata, data flows, and data models are types of data documentation.

Data management: Data management is the development, execution, and supervision of plans, policies, programs, and practices that deliver, control, protect, and enhance the value of data and information assets throughout their lifecycles. Data is a type of information.

Data quality: A measure of the data's reliability, including its accuracy, completeness, timeliness, consistency, validity, uniqueness, and interoperability.

Data register: A set of data that contains authoritative data and follows a specific standard to ensure quality, interoperability, and data sharing.

Government information: As defined in Part 1 of the Information Management Act. Government information includes both data and records.

High value data: Data that holds significant business value, enabling decision-making in support of programs, services, evaluation, and accountability requirements benefiting a high number of users. This includes data that supports critical services or data of public interest or permanent value (e.g., critical information and authoritative data).

Information: Any collection of data that is processed, analyzed, interpreted, classified, recorded, or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form. Information includes both data and records (MGIP, p.9).

Information management (IM): The means by which an organization plans, collects, organizes, governs, protects, uses, controls, disseminates, exchanges, maintains and disposes of its information; as well as any means through which the organization ensures its information's value is identified and that the information is used to its fullest extent, including the facilitation of efficient discoverability of information (MGIP, p.9).

Lifecycle: The life span of information from its creation or receipt and use, through to its final disposition: destruction, transfer to the government archives or alienation. (MGIP, p.10).

REVISION HISTORY

Version	Date	Notes
1.0	Jul. 7, 2023	Approved by Hayden Lansdell, ADM, BC Data Service
1.0.1	Oct. 16, 2023	Fixed broken link to Core Metadata Standard
1.0.2	Apr. 17, 2024	Removed link to the API Guidelines