4.12 Information Sharing Policy

Policy Statement

This policy promotes a culture of shared information for improved decision-making, policy, and business outcomes. It encourages sharing information unless there is a legitimate reason not to and sets out consistent best practice for appropriate information sharing. It is concerned with structured collections of information (e.g., data sets), as opposed to the sharing or release of individual documents which are better handled under the *Freedom of Information and Protection of Privacy Act* (FOIPOP).

It does not replace or override any current legislation or policy governing information access or protection. Where personal information is involved, sharing must be in accordance with FOIPOP, the *Personal Information International Disclosure Protection Act* (PIIDPA), and other department or information-specific legislation (e.g., *Personal Health Information Act*). It also does not override any contracts, agreements, or legislation governing confidential information. It does, however, encourage aggregating, de-identifying, or otherwise de-sensitizing information to allow for sharing and optimizing the value of government information.

Information held by government is a corporate asset that should be shared with any program, department, other government, or partner organization where the sharing would enhance services or inform operations unless access is limited by law, contract, or policy. Appropriate information sharing enables and supports coordinated and seamless services and optimizes decision-making by having access to a broader range of information thereby helping to improve community and client outcomes.

While the policy is primarily concerned with sharing information internally or with partners for better business, it also encourages identifying data that is appropriate for public distribution, and may be of interest to the public, and publishing it as open data. Greater accessibility enhances the social and economic benefit of government information and data, and creates a participatory environment where citizens and businesses are engaged with government.

Definitions

AGGREGATING

Expressing data in a summary form, with individual identifiers removed, for purposes such as statistical analysis.

CONFIDENTIAL INFORMATION

Information that is non-public and intended to be kept secret such as:

- Secret recipes, processes, formulas, and inventions still under development and not patented
- Secret data or information used in business such as customer, supplier, and employee lists
- Information that the receiving party agrees, knows, or reasonably should know was supplied in confidence
- Information that may result in undue financial gain or loss to a third party
- Advice to ministers
- Provincial budget prior to public release
- Draft legislation or regulations prepared for Executive Council
- Information that may harm law enforcement proceedings
- Privileged information between lawyers and their clients

DATA

Facts or figures used for analysis or calculation, based on observation or record-keeping, and often in a form suitable for storage in or processing by a computer. Data, as opposed to information, is raw, unprocessed, and lacks meaning until given context.

DATA STEWARD

A business representative who is responsible for determining, describing, and enforcing the business rules and definitions for data assets, including determining access, metadata, quality, and compliance requirements. The data steward should not be confused with IT representatives who are responsible for safe custody, transport, storage of the data and the implementation of business rules.

DE-IDENTIFIED INFORMATION

As described in 3(g) of the *Personal Health Information Act*, "information that has had all identifiers removed that

i. identify the individual, or
ii. where it is reasonably foreseeable in the circumstances, could be utilized, either alone or with other information, to identify the individual;"

INFORMATION
Knowledge obtained from investigation, study, or communication. Information is data that is processed, organized, and given context to make it useful. It is data that has been interpreted to clarify the underlying meaning.

PERSONAL INFORMATION
As defined in clause 3(1)(I) of the *FOIPOP Act*, "recorded information about an identifiable individual, including:

i. the individual's name, address or telephone number,
ii. the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
iii. the individual's age, sex, sexual orientation, marital status or family status,
iv. an identifying number, symbol or other particular assigned to the individual,
v. the individual's fingerprints, blood type or inheritable characteristics,
vi. information about the individual's health-care history, including a physical or mental disability,
vii. information about the individual's educational, financial, criminal or employment history,
viii. anyone else's opinions about the individual, and
ix. the individual's personal views or opinions, except if they are about someone else;"

REDACTING
Editing a document prior to release by obscuring or removing personal or sensitive information.

SENSITIVE INFORMATION
Non-public information where access may be restricted to certain individuals or positions. If used in any way other than intended, it could adversely affect security or the internal and/or external affairs of the province. The information may only be sensitive for a particular period of time. Some examples include:

- The locations of endangered species
- System vulnerability reports or security audits
- Employee access card logs or IT server logs
- Draft policies and reports prior to approval or publication
- Preliminary planning documents/information
- Building plans where security vulnerabilities may be exposed

Policy Objective

This policy was designed to:

- Promote information sharing by creating an environment where information is shared unless there is a legitimate reason not to, ensuring the right balance between information access and protection.
- Establish a culture where information is treated as a corporate asset and employees seek opportunities for sharing it to inform decision-making, reduce duplication and cost, and improve service delivery and outcomes for business and citizens.
- Establish a comprehensive and consistent practice for information sharing between departments, other governments, and partner organizations with whom government works collaboratively.
- Set out the rules, values, and principles for information sharing.
- Give employees the confidence to understand when information can be shared, with whom, and how.
- Enhance the social and economic benefit of government information and data.
- Empower citizens and businesses to create value from government data by proactively publishing data suitable for public distribution as open data.

Application

The policy applies to:

- All government departments, agencies, boards, and commissions categorized as Category I or II entities in the Corporate Administrative Policy Manuals Policy. Category III entities are recommended, but not required, application.
- All information and data under the custody or under the control of the province. The policy is concerned with structured collections of information (i.e., data sets), as opposed to the sharing or release of individual documents which are better handled under the *Freedom of Information and Protection of Privacy Act* (FOIPOP).

Policy Directives

A. Departments are to identify collections of information (e.g., data sets) over which they have primary responsibility and to identify data stewards responsible for administration, quality, and as contact points for information sharing requests.

B. Departments are responsible for periodic reviews of security, quality, accessibility, and access and use conditions of the data sets for which they have primary responsibility.
C. A list of government information assets (e.g., data sets) is to be maintained in the corporate information asset directory and must include descriptive elements such as the appointed steward, any known limitations on quality, and any legislative or legal requirements or restrictions.
D. Departments are to identify information assets (e.g., data sets) that are shareable and note that they are shareable in the corporate information asset directory.
E. Departments/program areas must consider the broader needs of government and seek opportunities to share information for joint program and service outcomes, and improved decision-making.
F. Departments/program areas must consider not only their immediate information requirements but also identify other potential users and uses so they can design and manage the information or information systems accordingly, including designing systems to import and export data in formats that support sharing.
G. Departments are to align with standard definitions and formats for information commonly shared between programs, departments, other governments, and partner organizations, in accordance with corporate standards.
H. Prior to creating new information assets, departments are to determine if the information required can be sourced from an existing collection within government while still meeting legislative requirements for privacy and confidentiality.
I. Data that may be of interest or useful to the public, and is appropriate for public distribution, is identified and proactively published as open data to enable citizens and sectors to create value from government data in accordance with government's Open Data Policy or Open Data requirements.
J. The Guidelines for Distribution and Sale of Government-Held Information are to be consulted when considering using commercial avenues for the distribution or sale of government information.
K. Privacy, confidentiality, and restricted access requirements must be met but must not become the inhibitor for limiting information sharing when it is permissible to do so.
L. When personal information is requested, aggregating, de-identifying, or redacting identifying data or information must be considered prior to denying the request.

M. When aggregating, de-identifying, or redacting information/data or combining or comparing data sets, the information/data must not become identifiable.

N. When sharing non-public information outside of a department, information sharing agreements must be developed and approved in accordance with the Information Sharing Permissions Framework or in accordance with law.

O. Exchanges of information within a department do not require an information sharing agreement but depending on the nature and sensitivity of the information, program areas may choose to prepare an agreement or to follow an internal departmental information sharing process.

P. When making an information sharing request, originating and receiving parties are to agree on a reasonable timeline for receiving the data so as to ensure that the information remains relevant for the purpose.

Q. Originating and receiving parties have a duty to discuss practices such as collection methods, quality controls, and the intended purpose of the sharing to ensure the receiving party/parties have the contextual information needed to use the information appropriately.

R. The information held by the originating department must be considered the official version unless the information sharing agreement states otherwise.

S. Requesting parties do not have the right to reproduce, market, or distribute information beyond the original agreement without the approval of the originating department(s).

T. Originating departments should develop and provide liability disclaimers appropriate for the information being disseminated.

U. In the case of a dispute over whether or not information can or should be shared, the Deputy Minister(s) or delegates(s) of the originating department(s) makes the final decision.

Accountability

A. Deputy heads or delegates(s) will:

- Ensure implementation of this policy and supporting materials;
- Encourage information sharing by promoting a culture where information is shared to optimize decision-making, enable greater collaboration, and to improve service delivery and outcomes for business and citizens.
- Approve information sharing agreements when information is shared outside of the department;
- Resolve disputes over whether or not information can or should be shared.

B. Senior Management will:

- Ensure information assets (e.g., data sets) over which the department has primary responsibility have been identified;
- Ensure information stewards are identified and their responsibilities explained and documented;
- Ensure information sharing agreements are developed where required and have undergone legal review.

C. The Corporate Information Management Program will:

- Lead the development and coordinate the on-going maintenance and updating of the corporate information asset directory;
- Provide advice, tools, and support for departmental programs on information sharing;

D. All employees will:

- Ensure they understand the policy and seek information sharing opportunities in compliance with the policy directives.

Monitoring

Departments are responsible for the consistent implementation and monitoring of the policy.

The Department of Internal Services will consult periodically with departments to receive feedback regarding the relevancy, usefulness, and effectiveness of the policy and materials provided to support the policy and make policy updates and revisions as required.

References

Freedom of Information and Protection of Privacy Act
Personal Information International Disclosure Protection Act
Personal Health Information Act
Privacy Review Officer Act

Related Documents

Privacy Policy
Website Privacy Policy
Information Management Policy

Open Data Policy
Information Sharing Agreement Template
Information Sharing and Privacy Good Practice Guide and Decision Chart
Information Sharing Permissions Framework
Guidelines for the Distribution and Sale of Government-Held Information

Enquiries

Director, Corporate Information Management Program
Information, Communications, and Technology Services Branch
Department of Internal Services
(902) 424-2915

Approval date:	***April 26, 2017***	Effective date:	***May 1, 2018***
Approved by:	***Treasury and Policy Board***	Administrative update:	