Table of Contents

1.0 Introduction .................................................................................................................................................. 3
  1.1 Scope ................................................................................................................................................. 3
  1.2 Effect ................................................................................................................................................... 3
  1.3 Legal Considerations .............................................................................................................................. 3
  1.4 Advice on this Policy ............................................................................................................................. 3

2.0 Policy Requirements ...................................................................................................................................... 4
  2.1 Accountability for Privacy Management ................................................................................................. 4
  2.2 Education and Awareness ....................................................................................................................... 5
  2.3 Privacy Impact Assessments .................................................................................................................... 6
  2.4 Agreements ............................................................................................................................................ 7
  2.5 Personal Information Inventories and Directory ..................................................................................... 8
  2.6 Privacy Breach Management and Compliance Monitoring ................................................................. 8
  2.7 Foreign Demands for Disclosure ........................................................................................................... 9
  2.8 Service Provider Management ............................................................................................................... 9

3.0 Summary of Roles and Responsibilities ........................................................................................................ 10

Appendix A – Glossary ........................................................................................................................................... 11

Appendix B – Links to Key Resources ............................................................................................................. 13
1.0 Introduction

The Government of British Columbia continually strives to enhance its interactions with citizens by setting new standards for service delivery in British Columbia. To meet this objective, the government must handle personal information of individuals, which must be collected, used, disclosed, stored and destroyed with due care. Government must be diligent in ensuring that processes are in place to protect personal information and to use it in a privacy-enhancing manner.

The Freedom of Information and Protection of Privacy Act (FOIPPA) mandates how personal information may be collected, used and disclosed by public bodies in British Columbia. The Privacy Management and Accountability Policy (PMAP) is government’s corporate approach to privacy management. The PMAP sets the framework for privacy to be a foundational component of all of government’s operations. It identifies the mandatory assessment tools and agreements that must be completed by ministries; reporting and audit requirements; and the policies and procedures that must be followed by ministries to ensure compliance with FOIPPA.

The PMAP provides direction regarding accountability for privacy management requirements including clearly articulating the roles and responsibilities of government’s ministries, Ministry Privacy Officers (MPOs), the Corporate Information and Records Management Office (CIRMO) and employees. The Privacy, Compliance and Training Branch (PCT) within CIRMO is the BC government’s central privacy office. This framework will strengthen government’s ability to protect the privacy of individuals’ personal information, and ensure that all ministries are compliant with the privacy requirements of FOIPPA and managing their personal information holdings in the most efficient manner.

1.1 Scope

The PMAP applies to all government ministries.

1.2 Effect

The requirements and accountabilities of this policy take effect immediately upon publication of the policy, with the exception of requirements related to relevant policies or guidelines not yet in place. When published, the related policies and guidelines will set out relevant effective dates.

1.3 Legal Considerations

FOIPPA protects personal privacy by prohibiting the unauthorized collection, use, disclosure, storage and destruction of personal information by government ministries and other public bodies. It is important to note that the PMAP does not replace or limit a ministry’s obligations under FOIPPA; rather the PMAP supports compliance with the privacy requirements of the Act. Ministries must ensure they meet all of their obligations under FOIPPA.

1.4 Advice on this Policy

Advice on the PMAP can be obtained from the Privacy, Compliance and Training Branch at 250-356-1851 or privacy.helpline@gov.bc.ca.
2.0 Policy Requirements

2.1 Accountability for Privacy Management

Deputy Ministers

2.1.1 Deputy Ministers must designate an individual responsible for privacy within their respective ministry and provide the contact information of this individual to the Corporate Information and Records Management Office (CIRMO). This individual will be designated the Ministry Privacy Officer (MPO). Deputy Ministers may, at their discretion, designate an additional Ministry Privacy Officer for a specific area within their ministry that provides corporate services for the BC Government (e.g. Public Service Agency, Government Communications and Public Engagement).

2.1.2 Deputy Ministers must use a FOIPPA Delegation Instrument if they wish to delegate any duties, powers or functions of the head under FOIPPA to the MPO or any other person. The Deputy Minister may perform this duty as head of the public body as per section 23 of the Interpretation Act.

Ministry Privacy Officers

2.1.3 MPOs may delegate any roles and responsibilities assigned to them under the PMAP using the PMAP Delegation Instrument, but remain accountable as the single point of contact for CIRMO.

2.1.4 MPOs must maintain any current FOIPPA Delegation Instruments for their ministry and provide updated copies to CIRMO.

2.1.5 MPOs must develop ministry specific policies and procedures, where necessary, to support this policy or compliance with FOIPPA. Any such ministry specific policies must be submitted to CIRMO for review.

2.1.6 MPOs must communicate any changes to the PMAP to relevant ministry Employees.

2.1.7 MPOs must consult with CIRMO before any engagement with the Office of the Information and Privacy Commissioner (OIPC) on matters relating to privacy and must include CIRMO in any engagement with the OIPC.

2.1.8 MPOs must inform CIRMO when their ministry has been contacted by the OIPC on matters relating to privacy.

Employees

2.1.9 Employees must comply with the PMAP and other privacy-related policies, guidelines and templates developed by CIRMO.

2.1.10 Employees must consult with CIRMO before any engagement with the OIPC on matters relating to privacy and must include CIRMO in any engagement with the OIPC.
2.1.11 Employees must inform CIRMO when their ministry has been contacted by the OIPC on matters relating to privacy.

*Corporate Information and Records Management Office*

2.1.12 CIRMO must review the PMAP annually with input from MPOs and other stakeholders, update as appropriate and inform MPOs of all significant changes.

2.1.13 CIRMO must establish and chair a Privacy Management Community of Practice to facilitate dialogue between the MPOs, CIRMO, and other interested parties.

2.1.14 CIRMO must provide orientation for new MPOs regarding their role and responsibilities under the PMAP.

### 2.2 Education and Awareness

*Ministry Privacy Officers*

2.2.1 MPOs must develop, in collaboration with CIRMO:

- i. Ministry-specific privacy training to support the PMAP, as required; and
- ii. Ministry-specific privacy training to support employees using information systems and programs that involve the handling of high-risk or sensitive personal information within their Ministry.

2.2.2 MPOs must ensure that mandatory training referred to in s.2.2.5 and 2.2.6 is taken by all Employees, as applicable.

2.2.3 MPOs must put a process in place for documenting Service Providers and volunteers who have access to Personal Information so that training requirements referred to in s.2.2.6 can be properly applied.

2.2.4 Once Ministry-specific training referred to in s.2.2.1 is developed, MPOs must ensure that the training is completed by all appropriate Employees within 6 months of working with an information system or program that involves the handling of high-risk or sensitive personal information.

*Employees*

2.2.5 Employees must complete training relevant to their job on the appropriate collection, use, disclosure, storage and destruction of personal information as prescribed by CIRMO. The IM117 course offered through the Public Service Agency may be applied towards this requirement.

2.2.6 Employees who are Service Providers and/or volunteers who collect or create personal information must complete prescribed privacy training on the appropriate collection, use, disclosure, storage and destruction of personal information, unless granted an exemption by
CIRMO. This training must be completed prior to providing any service that involves personal information. Training referred to in s.2.2.5 may be applied towards this requirement (where it has been documented).

2.2.7 An exemption to s.2.2.5 and 2.2.6 may be granted in extenuating circumstances if it is determined by CIRMO that equivalent training is completed in place of CIRMO-developed training.

2.3 Privacy Impact Assessments

Ministry Privacy Officers

2.3.1 MPOs must ensure that Privacy Impact Assessments (PIAs) are completed where necessary. A PIA is not complete until it has been fully signed by all required parties as set out in the PIA Directions. PIAs must be completed before the start of any new or updated enactment, system, project, program or activity.

2.3.2 MPOs must support the development of PIAs that accurately represent the program/initiative under assessment and are completed in accordance with the PIA Directions prior to submission to CIRMO.

2.3.3 MPOs must develop, maintain and review internal processes to ensure completion of PIAs and the mitigation of risks identified in PIAs within their ministry.

2.3.4 MPOs must support the reasonable mitigation of privacy risks identified through the PIA process.

2.3.5 MPOs must ensure that a copy of each completed and signed PIA is provided to CIRMO for retention and for entry into the Personal Information Directory (PID), and must do so in accordance with the PID Policy (once drafted).

2.3.6 An MPO may be granted an exemption for PIA accountability, at the discretion of CIRMO determined on a case-by-case basis. Exemption does not preclude an MPO from remaining involved.

Employees

2.3.7 Employees must conduct PIAs in accordance with the PIA Directions as issued by the Minister responsible for FOIPPA, and must only use the templates developed by CIRMO.

2.3.8 Employees must conduct PIAs during the development of any proposed enactment, system, project, program, or activity of the ministry, or any proposed changes to an enactment, system, project, program or activity.

2.3.9 Employees must provide PIAs to their MPO to enable MPOs to fulfill their obligations under 2.3.2., and then the PIA must be submitted to CIRMO for review and comment. A PIA is not complete until it has been fully signed by all required parties as set out in the PIA Directions. PIAs must be completed before the start of the proposed enactment, system, project, program or activity.
2.3.10 Employees must work with their MPO to reasonably mitigate privacy risks identified through the PIA process.

2.3.11 As stated in 2.3.6, under certain circumstances, at the discretion of CIRMO, Employees may work directly with PCT instead of their MPO. Such cases will be examined on a case-by-case basis and in consultation with their MPO.

**Corporate Records and Information Management Office**

2.3.12 CIRMO must review and comment on all PIAs submitted by ministries.

2.3.13 CIRMO must maintain the PIA Directions.

**2.4 Agreements**

*Ministry Privacy Officers*

2.4.1 MPOs must ensure completion of all Information Sharing Agreements (ISAs) as required for their ministry in accordance with the ISA Directions.

2.4.2 MPOs must support completion of all Common or Integrated Program/Activity Agreements (CPAs or IPAs) as required for their ministry, in accordance with section 69 of [FOIPPA](#) and section 12 of the [FOIPP Regulation](#).

2.4.3 MPOs must support completion of all Research Agreements (RAs) as required for their ministry in accordance with section 35 of FOIPPA.

2.4.4 MPOs must ensure any ISAs, RAs, CPAs, and IPAs are updated when they are made aware of material changes to an initiative.

2.4.5 MPOs must develop, maintain and review internal processes to ensure completion of accurate ISAs, RAs, CPAs and IPAs within their ministry.

2.4.6 MPOs must report all completed ISAs, including IPAs and CPAs, to CIRMO for entry into the PID and do so in accordance with the PID Policy (*once drafted*).

2.4.7 MPOs must keep an inventory of all RAs entered into by their ministry.

*Employees*

2.4.8 Employees must complete ISAs in accordance with the ISA Directions (*once drafted*), unless granted an exemption by CIRMO. An ISA is not complete until it has been fully signed by all required parties.

2.4.9 Employees must complete RAs in accordance with section 35 of FOIPPA.
2.4.10 Employees must complete CPAs and IPAs in accordance with section 69 of FOIPPA and section 12 of the FOIPP Regulation and in accordance with the ISA Directions (once drafted).

_Corporate Records and Information Management Office_

2.4.11 CIRMO must maintain the ISA Directions.

2.5 **Personal Information Inventories and Directory**

_Ministry Privacy Officers_

2.5.1 MPOs must ensure that their ministry’s personal information holdings and any other required details are listed in a Personal Information Inventory within one year of the Personal Information Inventory Policy (once drafted) being published.

2.5.2 MPOs must report Personal Information Banks (PIBs) that result from new enactments, systems, projects, programs, or activities of a ministry to CIRMO for entry into the Personal Information Directory (PID), in accordance with the PID Policy (once drafted).

2.5.3 MPOs must ensure the information contained in the PID for their respective ministry is accurate and updated as needed.

2.5.4 The MPO for the Ministry of Health must ensure that the required information regarding Health Information Banks (HIBs) is submitted to CIRMO for entry into the PID.

_Corporate Information and Records Management Office_

2.5.5 CIRMO must consult with ministries and establish a mechanism for ministries to document details of their personal information holdings as required by the Personal Information Inventory Policy (once drafted).

2.5.6 CIRMO must manage and publish the PID. This includes revising entries with updated information identified and provided by the MPOs.

2.6 **Privacy Breach Management and Compliance Monitoring**

_Ministry Privacy Officers_

2.6.1 MPOs must complete ministry practice reviews of their privacy management practices in accordance with the Information Management Practice Review Policy.

_Employees_

2.6.2 Employees must immediately report actual or suspected Privacy Breaches, including privacy complaints as per the Information Incident Management Policy.
* Please refer to the Information Incident Management Policy for more information on the requirements for responding to information incidents, including privacy breaches and the Information Management Practice Review Policy for more information regarding compliance assessments.

2.7 Foreign Demands for Disclosure

Employees

2.7.1 Employees receiving Foreign Demands for Disclosure must immediately notify CIRMO in the manner and form directed by CIRMO.

2.8 Service Provider Management

Ministry Privacy Officers

2.8.1 MPOs must ensure that Service Providers and volunteers referred to in s. 2.2.6 complete the relevant training.

Employees

2.8.2 Employees who prepare or manage contracts must include the standard Privacy Protection Schedule in all contracts that involve personal information in the custody or under the control of the public body, except where an alternate version is approved by CIRMO.

2.8.3 Employees who prepare or manage contracts must inform MPOs of all Service Providers and volunteers that have access to personal information within the ministry’s custody or control.
3.0 Summary of Roles and Responsibilities
This section broadly summarizes the requirements in section 2.0 by role.

Deputy Ministers
Deputy Ministers are responsible for:

- Ensuring that the PMAP is communicated to all Employees in their respective ministry.
- Designating a MPO for their ministry.
- Supporting the continuous improvement of privacy practices and the responsible collection, use, disclosure, storage and destruction of personal information in their ministry

Corporate Information and Records Management Office (CIRMO)
The Corporate Information and Records Management Office is responsible for:

- Providing guidance, expert advice and recommendations on privacy, including on the implementation of PMAP and the development of ministry specific privacy policies.
- Developing and providing training for employees regarding personal information and privacy, including mandatory privacy training courses.
- Acting as government’s liaison with the OIPC on privacy related matters.
- Maintaining the Privacy Management Community of Practice.
- Reviewing and assessing compliance with privacy policies, procedures, and legislation.
- Coordinating, investigating, and/or resolving actual or suspected information incidents (including privacy breaches).
- Reviewing and commenting on all Privacy Impact Assessments (PIA) submitted.
- Managing the Personal Information Directory.

Ministry Privacy Officers (MPOs)
Ministry Privacy Officers are responsible for:

- Implementing and managing compliance with the Privacy Management and Accountability Policy, and its supporting policies.
- Promoting privacy awareness within their ministry, including ensuring mandatory privacy training is taken by all employees and that ministry specific training and policy is developed as appropriate.
- Managing and coordinating the completion of Privacy Impact Assessments as appropriate.
- Supporting completion of research agreements, information sharing agreements, and common or integrated program/activity agreements and ensuring they are maintained and inventoried as appropriate.
- Correcting any inaccurate information in the Personal Information Directory.

Employees
Employees are responsible for:

- Complying with this policy and for seeking direction from their supervisors if they have questions.
Appendix A – Glossary

**Common or Integrated Program or Activity** means a program or activity that

(a) provides one or more services through
   (i) a public body and one or more other public bodies or agencies working collaboratively, or
   (ii) one public body working on behalf of one or more other public bodies or agencies, and
(b) is confirmed by regulation as being a common or integrated program or activity.

**Contact Information** means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

**Employee** means an individual working for the Government of British Columbia.

**FOIPPA Delegation Instrument** means the tool by which the head of a public body authorizes an Employee within the public body or another public body to exercise one or more of the head's authorities or decision-making powers under FOIPPA. The person delegating the authority remains responsible and accountable for all actions and decisions made under that delegation.

**Foreign Demand for Disclosure** means a subpoena, warrant, order, demand or request that is

(a) from a foreign court, an agency of a foreign state or another authority outside Canada, and
(b) for the unauthorized disclosure of personal information to which FOIPPA applies.

**Information Incident** means a single or a series of events involving the collection, storage, access, use, disclosure, or disposal of government information that threaten privacy or information security and/or contravene law or policy.

**Information Sharing Agreement** means an agreement between a public body and one or more of the following:

(a) another public body;
(b) a government institution subject to the Privacy Act (Canada);
(c) an organization subject to the Personal Information Protection Act or the Personal Information Protection and Electronics Documents Act (Canada);
(d) a public body, government institution as defined in applicable provincial legislation having the same effect as FOIPPA;
(e) a person or group of persons; or
(f) an entity prescribed in the FOIPP Regulation

that sets conditions on the collection, use or disclosure of personal information by the parties to the agreement.

**Ministry Privacy Officer** means the designated individual from each ministry responsible for privacy and the implementation of this policy within their ministry.

**Personal Information** means recorded information about an identifiable individual other than contact information.

**Personal Information Directory** means the public-facing database used to document the management of personal information holdings of government and to assist the public in identifying the location of personal information about them held by government.
**Personal Information Inventory** means a listing of all personal information holdings held by a ministry.

**Privacy Breach** means the collection, storage, access, use, disclosure, or disposal of personal information that is not authorized by Part 3 of the *Freedom of Information and Protection of Privacy Act*. A privacy breach is a type of information incident.

**Privacy Impact Assessment** means an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 (Protection of Privacy) of FOIPPA.

**PMAP Delegation Instrument** means the tool by which an MPOs authorizes another Employee within the public body or another public body to exercise one or more of their authorities or decision-making powers under this policy. The person delegating the authority remains responsible and accountable for all actions and decisions made under that delegation.

**Privacy Protection Schedule** means a schedule completed and attached to any contract between the government and a Service Provider that involves personal information. Its purpose is to:

(a) enable the Province to comply with its statutory obligations under FOIPPA with respect to personal information; and  
(b) ensure that the Service Provider is aware of and complies with its statutory obligations under FOIPPA with respect to personal information.

**Research Agreement** means an agreement setting out the approved conditions under which personal information is disclosed for research purposes, pursuant to s.35 of FOIPPA.

**Service Provider** means a person retained under contract to perform services for the Government of British Columbia.

**Unauthorized Disclosure of Personal Information** means disclosure of, production of or the provision of access to personal information to which FOIPPA applies, if that disclosure, production or access is not authorized by FOIPPA.
Appendix B – Links to Key Resources

Freedom of Information and Protection of Privacy Act (FOIPPA):

FOIPPA Delegation Instrument:
https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/resources/templates/foippa_delegation_instrument.docx

Freedom of Information and Protection of Privacy Regulation:

Information Incident Management Policy:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/resources

ISA Directions:
Under development

ISA Template:
http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/resources/templates/information_sharing_agreement_template.doc

Ministry Privacy Officer Directory:
www.gov.bc.ca/privacyofficers

Personal Information Directory (via DataBC):
http://catalogue.data.gov.bc.ca/dataset/bc-personal-information-directory-pid

Personal Information Inventory Policy:
Under development

Personal Information Directory (PID) Policy:
Under development

Information Management Practice Review Policy:
Under development

Privacy Impact Assessment Directions, Template and Guidelines:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments

Privacy Protection Schedule:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/agreements-contracts/privacy-protection-schedule

PMAP Delegation Instrument:
Under development

Sample Research Agreement Form: