TOWN OF GRIMSHAW

PRIVACY MANAGEMENT PROGRAM

TABLE OF CONTENTS

Introduction

Purpose 2
Scope 2
Definitions 2

Governance & Accountability 3
Policy 4
Procedure 7
Education & Awareness 10
Roles & Responsibilities 10
Authority to Act 11
Related Documents 11
Contact 11
Review 11

Introduction

Purpose

A strong and accessible PMP will help ensure personal information is handled with care and transparency and that privacy risks are identified and managed appropriately and proactively. The Town is committed to strengthening public trust and meeting our legal obligations.

Scope

This program applies to all individuals who collect, use, or disclose personal information on behalf of the Municipality, whether through direct employment (staff), appointment (elected officials, volunteers and committee members), or contractual agreement (contractors & service providers).

Definitions

ATIA means the Access to Information Act.

POPA means the Protection of Privacy Act.

Personal Information means recorded information about an identifiable individual, as defined in POPA, and does not include business contact information where excluded by law.

Business Information means business contact information such as an individual's name, position title, business telephone number, business address, and business email address, where treated in accordance with applicable law.

Indirect Collection means collection of personal information from a source other than the individual the information is about, where authorized by POPA or another enactment.

Designate means the head of the public body, or a person authorized to act on behalf of the head in accordance with applicable law or delegation.

Privacy Officer means the individual designated by the Town to support the development, implementation, maintenance, and administration of the Town's privacy management program and related privacy processes.

Public Body means the Town of Grimshaw.

Town means the Town of Grimshaw

Governance & Accountability

The Town is accountable for personal information in its custody or under its control. Council provides governance oversight, and Administration is responsible for implementing this Privacy Management Program in day-to-day operations.

- **Head/Designate:** The Town will identify the head of the public body and any lawful delegations or designations in its bylaws, policies, or authorizing instruments, as applicable.
- **Privacy Officer:** The Privacy Officer supports compliance with POPA and ATIA, coordinates privacy advice, access and correction processes, complaint handling, training, and breach response.
- **Reporting:** The Town may report privacy, access, training, and breach management metrics internally or to Council as appropriate to support oversight and continuous improvement.
- **Training:** Employees, elected officials, volunteers, committee members, and service providers with access to personal information will receive privacy and security training appropriate to their roles.

Policy

1. **Collection of Personal Information**

   The Town of Grimshaw will collect personal information only where authorized by POPA or another enactment and only as reasonably necessary for an operating program or activity of the Town.

   a. where collection is expressly authorized by POPA, ATIA, another enactment, or a Town bylaw that lawfully authorizes the activity;
   b. for planning, administering, delivering, evaluating, or improving Town programs, services, and activities;
   c. for law enforcement or regulatory purposes, including the administration and enforcement of bylaws; and
   d. in connection with public meetings, hearings, delegations, and other processes where individuals choose to participate and the collection is authorized by law.

   Where required, the Town will collect personal information directly from the individual and provide an appropriate collection notice. The Town may collect personal information indirectly where authorized by POPA, another enactment, or with the individual's consent.

   a. where another enactment authorizes the indirect collection; and

b. where the information is collected for the purpose of a legal proceeding or other authorized purpose.

2. Use and Disclosure of Personal Information

The Town will use and disclose personal information only as authorized by POPA and, generally, only for the purpose for which it was collected or for a consistent purpose permitted by law.

a. with the individual's consent, where consent is an authorized basis;
b. to employees, elected officials, volunteers, committee members, contractors, or service providers where the information is reasonably required to carry out their authorized duties for the Town;
c. where disclosure is required or authorized by an enactment of Alberta or Canada;
d. to another public body or law enforcement agency where authorized for an investigation, law enforcement matter, or other legal purpose; and
e. to the Town's legal counsel where reasonably necessary for legal advice, litigation, or another authorized legal matter.

Note: Information provided for open meetings of Council or its committees may become part of the public record where authorized by law.
If you provide personal information for that purpose, it may be included in meeting materials, minutes, livestreams, recordings, or other records made available to the public in accordance with applicable law.
The Town will make reasonable efforts to limit unnecessary disclosure of personal information in public records while maintaining transparency obligations.
Individuals with legitimate personal safety concerns should contact the Town in advance to discuss whether alternative arrangements are available and lawful.

3. Safeguarding

The Town will make reasonable security arrangements to protect personal information in its custody or under its control against such risks as unauthorized access, collection, use, disclosure, modification, disposal, or destruction. Safeguards will be administrative, physical, and technical, and proportionate to the sensitivity, volume, and classification of the information.

4. Accuracy

The Town of Grimshaw will make every reasonable effort to ensure that personal information used for an administrative purpose affecting an individual is accurate and complete.

5. Access to Personal Information

Ways to access information from the Town of Grimshaw:

1. Individuals may contact the Town to request access to their own personal information in the custody or under the control of the Town.
2. Town employees seeking access to their own employment-related personal information may contact the Town office or the Privacy Officer for direction.

The Town will review your request to determine whether it can be handled as a routine request or whether it must be treated as a formal request under the Act.

a) If your request involves another person's personal information, or information otherwise protected under the Act, we may require you to submit a formal access request under the Act.
b) Once a formal request is received under ATIA, the Town generally has 30 business days to respond, subject to any extension or other requirement permitted by the Act.
c) Before we disclose any personal information, you will be required to verify your identity so we can confirm that the information is being released to the correct individual.
d) Please note that, in some circumstances, the Act may require us to refuse access, even to your own personal information.
e) If your request is a formal request under the Act, we will provide you with written reasons for our decision.

6. Correction of Personal Information

An individual who believes there is an error or omission in their personal information may request a correction in writing. If the Town agrees a correction is warranted, it will correct the information as appropriate. If the Town does not agree to the requested correction, it will annotate the record or otherwise manage the request as required by law.

7. Retention and Disposal of Personal Information

The Town and its service providers will retain and securely dispose of records containing personal information in accordance with applicable legislation, approved records retention and disposition schedules, operational requirements, and legal holds.

Where personal information has been used to make a decision directly affecting an individual, the Town will retain the information for at least one year after the decision, or for a longer period where required by law or approved records schedules.

When personal information is no longer required to be retained, it will be destroyed or otherwise disposed of securely and confidentially in accordance with Town procedures.

8. **Using the Town of Grimshaw Website**
   The Town's website automatically collects and stores the following information from visitors to the website:
   the internet protocol (IP) address and domain name used (the IP address is a numeric identifier assigned to either the individual's internet service provider or directly to the computer)
   - the type of browser and operating system
   - the date and time of the visit
   - the webpage(s) accessed
   - amount of time spent on each page

   This information is collected for website administration, security, performance monitoring, troubleshooting, analytics, and service improvement. The Town will not use this information to identify an individual unless authorized or required by law.

   Where individuals voluntarily provide personal information through email, forms, or other web services, the Town will collect, use, and disclose that information only for the purpose for which it was provided or as otherwise authorized by law.

9. **Links to Other Websites**
   The Town's website includes links to webpages operated by other organizations. These links are not intended to be referrals and are posted only for convenience. The Town will have no responsibility for, liability, or control over these links or websites. Please refer to the individual privacy policies and terms and conditions of use for external sites.

Procedure

Privacy Complaints and Breaches
Complaints about a privacy-related matter under this policy or under POPA should be submitted in writing to the Privacy Officer. The Town will review the complaint, determine the appropriate process, and respond in writing where required or appropriate.

Privacy Breach Reporting and Notification

1. Any suspected or confirmed privacy breach must be reported immediately to the Privacy Officer and the appropriate supervisor or designate, in accordance with Town procedures.

The Town will document, assess, contain, investigate, and respond to the incident without unreasonable delay.

2. Where a privacy breach creates a real risk of significant harm, the head of the public body or designate will, without unreasonable delay and as required by law, notify affected individuals, the Commissioner, and the Minister.

How to Notify

Direct Notifications— Affected Individuals

Notifications must include the following information:

- the name of the public body;
- the date on which the privacy breach came to the attention of the public body;
- a description of the privacy breach including, if known,
- the date on which or the period during which the privacy breach occurred, and
- a description of the nature of the personal information involved in the privacy breach;
- confirmation that the commissioner has been or will be notified of the privacy breach;
- contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;
- a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

Indirect Notifications—Affected Individuals

A notification may be given to an affected individual in an indirect manner if

a) the public body does not have accurate contact information for the affected individual,
b) the head of the public body reasonably believes that providing the notice directly to the affected individual would unreasonably interfere with the operations of the public body, or
c) the head of the public body reasonably believes that the information in the notification will come to the attention of the affected individual more quickly if it is given in an indirect manner.

If a notification must be given in an indirect manner, the notification must

a) be given by public communication that can reasonably be expected to reach the affected individual, and
b) contain the following information:
    - the name of the public body;
    - the date on which the privacy breach came to the attention of the public body;

- a description of the privacy breach including, if known,

a) the date on which or the period during which the privacy breach occurred, and
b) a description of the nature of the personal information involved in the privacy breach;

- confirmation that the commissioner has been or will be notified of the privacy breach;
- contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;
- a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

Notifications – Commissioner

A notification under section 37 (1) of the Act must be given to the commissioner in writing and must include the following information:

- the name of the public body;
- the date on which the privacy breach came to the attention of the public body;
- a description of the privacy breach including, if known,
    a) the date on which or the period during which the privacy breach occurred,
    b) a description of the nature of the personal information involved in the privacy breach, and
    c) an estimate of the number of affected individuals;
- contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individuals.

Not Required to Notify

a) The head of a public body is not required to notify an affected individual if notification could reasonably be expected to:
result in immediate and grave harm to the individual's safety or physical or mental health; or
b) threaten another individual's safety or physical or mental health.

Disregarding Requests

1. Where permitted by ATIA, the Town may disregard a request in the circumstances set out in the Act. If the Town decides to disregard a request, it will provide reasons and information about any available right of review, as required by law.

Privacy Impact Statements
Privacy impact assessments are required for new or significantly changed systems, projects, programs, services, activities, or technologies that involve the collection, use, disclosure, storage, analysis, matching, or other handling of personal information, where required by POPA and its regulations.
The Town will complete PIAs in the form (Schedule A attached) and manner required by law and will submit them for review and comment where submission is required.
Employees initiating a relevant change or initiative must consult the Privacy Officer early so privacy risks can be identified and addressed before implementation.

Service Provider Management
Where a service provider may access, collect, use, store, disclose, or otherwise handle personal information on behalf of the Town, the responsible department must ensure that contracts include privacy, confidentiality, security, records management, breach reporting, audit, and return or secure destruction requirements, as appropriate.

Information Sharing Agreements
Where the Town proposes a regular or systematic exchange of personal information with another organization, public body, or partner, the Town will assess the legal authority, privacy risks, safeguards, and operational requirements, and will use a written information-sharing agreement where appropriate.

EDUCATION AND AWARENESS

All Town of Grimshaw employees receive privacy and access training appropriate to their roles and responsibilities. Additional training is provided where duties involve higher-risk information, specialized systems, access requests, breach response, information sharing, or privacy impact assessments.
Additional training is given in the following circumstances:

- Employees handling what is considered high-risk or sensitive personal information electronically receive training related to information systems and their security, in coordination with the IT department
- Employees managing programs or activities receive training related to privacy impact assessments; and
- Employees managing common or integrated programs or activities receive training related to information sharing agreements.

ROLES AND RESPONSIBILITIES

Town Council:

- Approves policy and procedures.

Department Heads:

- Support and cooperate with the Privacy Officer in implementing the policy and in complying with POPA.

Privacy Officer/Designate:

- Responsible for the development, management and implementation of the Town's privacy management program including ongoing assessments and revisions.
- Coordinates employee training and education, including orientation and refresher training, and supports ongoing review and improvement of privacy practices.

AUTHORITY TO ACT

The head of the public body, and any designate acting under lawful authority, is responsible for ensuring compliance with this policy and with applicable privacy and access legislation.

RELATED DOCUMENTS

- Access to Information Act
- Protection of Privacy Act

ACCESS TO PERSONAL INFORMATION AND QUESTIONS REGARDING PRIVACY

Inquiries, complaints, correction requests, or access requests regarding personal information should be directed to the Town's Privacy Officer.

Privacy Officer, Town of Grimshaw
780-332-4626

For more information, contact the Office of the Information and Privacy Commissioner of Alberta.
The Town may amend this Privacy Management Program from time to time to reflect legislative, regulatory, operational, or organizational changes.

REVIEW

This policy shall be reviewed periodically and at least once every 3 years, or sooner if required due to legislative change, organizational change, audit findings, or material privacy risks.

Review Schedule:

Original Approval Date	Reviewed by Policy and Personnel Committee	Adopted by Council
N/A	June 4, 2026	

PRIVACY IMPACT ASSESSMENT

Protection of Privacy Act (POPA)

Section 26 of the Protection of Privacy Act and Section 7 of the Protection of Privacy (Ministerial) Regulation.

Disclaimer:

This document is not intended as, nor is it a substitute for, legal advice, and is not binding on the Information and Privacy Commissioner of Alberta. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization, custodian or public body. All examples used are provided as illustrations. The official versions of the laws the OIPC oversees and their associated regulations should be consulted for the exact wording and for all purposes of interpreting and applying the legislation. The Acts are available on the website of Alberta King's Printer.

Table of Contents

Introduction 3

Common Questions 4

Read Before Completing your PIA 6

A. General Information About the Public Body or Bodies, Existing PIAs, and the Project * 7

B. Details About the Project * 11

C. Information About Your Privacy Management Program (PMP) * 12

D. Identify Personal Information Involved and your Authority to Collect, Use or Disclose the Information* 12

E. Access, Correction, Accuracy, Retention, Disposition * 16

F. Protection of Information * 20

G. Service Providers * 26

H. Project Risk Assessment and Mitigation * 29

H1. General Risks (to be completed for all PIA submissions) * 30

H2. Risks Associated with Cloud Computing 32

H3. Risks Associated with Research 34

Appendix A. Data Matching 35

Appendix B. Common or Integrated Program or Service 40

Appendix C. Use of Automated Systems or Other Forms of Innovative Technology 44

Appendix D. PIA Cover Letter * 47

Appendix E. PIA Submission Checklist * 48

Introduction

Section 26 of the *Protection of Privacy Act* (POPA) requires a public body to prepare a privacy impact assessment (PIA) in prescribed circumstances and, if required by the regulations, submit it to the Commissioner in accordance with the regulations. In addition, as part of the Commissioner's responsibility to monitor how POPA is administered to ensure that its purposes are achieved, the Commissioner may, as described in section 27(1)(j) of POPA, request a copy of a public body's PIA.

Section 7(1) of the *Protection of Privacy Act (Ministerial) Regulation* (M-Regulation) requires a public body to prepare a PIA with respect to a new, or a substantial change to an existing, administrative practice, program, project or service that involves the collection, use or disclosure of personal information if one or more of the following factors requiring the submission of a PIA to the Commissioner apply:

(a) A practice, program, project or service will collect, use or disclose personal information deemed to be of high sensitivity. Section 1 of the M-Regulation deems biometric information about an individual, financial information about an individual, personal information respecting a minor, senior or vulnerable individual to be of high sensitivity.

(b) A practice, program, project or service will involve the personal information of a significant percentage of the population the public body serves.

(c) A practice, program, project or service will involve data matching between two or more public bodies. Section 1(f) of POPA defines "data matching" as linking personal information between two or more databases or other electronic sources of information.

(d) A practice, program, project or service is part of a common or integrated program or service. Section 1(d) of POPA defines "common or integrated program or service" in relation to a public body to mean a program or service planned, administered, managed, monitored or evaluated by (i) the public body working collaboratively with one or more other public bodies, or (ii) another public body working on behalf of (A) the public body, or (B) the public body and one or more other public bodies.

(e) A practice, program, project or service involves the development or use of innovative technology.

Public bodies are to use this template document when submitting their POPA PIAs to the Office of the Information and Privacy Commissioner (OIPC).

Common Questions

1. What is a PIA?

Generally, a PIA maps the flow of information in a proposed system or practice or project and identifies the legal authority permitting it. A PIA also identifies privacy and security risks and associated mitigating controls.

2. Why is a PIA important, or in some cases, required?

Conducting a PIA prior to implementing a new, or a substantial change to an existing, information system, administrative practice, program, project or service, which will involve the collection, use or disclosure of personal information, assists a public body in identifying and addressing potential privacy and security risks that may occur when processing personal information as part of an electronic information system, administrative practice, data matching or in other circumstances where risks to privacy may result from the processing. It also allows the public body to look at and evaluate information flows to determine if the collection, use and disclosure of the personal information complies with POPA.

3. What if I am not sure if I am required to submit a PIA to the Commissioner?

If a public body is unsure whether it is required to complete a PIA or to complete and submit a PIA to the Information and Privacy Commissioner, the public body should use the PIA Submission Assessment Tool for assistance.

4. Is a public body required to complete PIAs without submitting them to the Commissioner?

Yes, a public body is required to complete PIAs under section 7(1)(a) of the M-Regulation. However, a public body is not required to submit PIAs conducted under 7(1)(a) of the M-Regulation to the Commissioner, but the Commissioner can request copies of those PIAs under section 27(1)(j) of POPA.

5. Can a public body use this PIA template to complete its own PIA pursuant to section 7(1)(a) of the M-Regulation?

Yes, the OIPC recommends that public bodies use this template for all POPA-related PIAs. For PIAs that must be submitted to the Commissioner under POPA, it is mandatory to use this template. Since the Commissioner can request these PIAs, it is important that the PIAs are completed to meet the PIA requirements under POPA, which is the foundation of this template.

6. What if I am unsure how to answer a question in the PIA template?

This template has a completion guide. The guide assists public bodies in completing this PIA template by providing explanations or clarifications, where necessary, for each question asked in the template and by describing what is expected of the public body in each question. We recommend that you complete the PIA template while consulting the **POPA PIA Template Completion Guide**.

If you cannot find answers to your questions in the guide, you may contact the OIPC at **780-422-6860 or 1-888-878-4044 (toll free) or by email at generalinfo@oipc.ab.ca**.

7. This template looks so complicated! Do I have to fill it out completely or to this level of detail?

Section 7(3) of the M-Regulation says a privacy impact assessment must provide a level of detail commensurate with the complexity of the practice, program, project or service that the privacy impact assessment relates to. Using this template when preparing a PIA will assist a public body in meeting this requirement. Don't be intimidated! If you have questions, you can refer to the guide or call our office for assistance. The template has been designed such that it is easy to complete.

Not all sections of this template may apply for a specific project. Consider identifying the sections that apply to the project before completing the PIA.

8. Who is authorized to sign off on POPA PIAs?

Given that section 26(1) of POPA requires a public body to prepare a PIA in prescribed circumstances and, if required by the regulations, submit it to the Commissioner in accordance with the regulations, the head of a public body is legally required to sign off on POPA PIAs. However, section 55(1) of POPA authorizes the head of a public body to delegate to any person any power, duty or function of the head under the Act, except the power to delegate under this section. Section 55(2) requires that a delegation under subsection (1) be in writing and may contain any conditions or restrictions the head of the public body considers appropriate. To this end, the Designate of a public body may sign off on the public body's PIA if that Designate has been delegated such a power. A copy of the delegation instrument should be included with the PIA.

Read Before Completing your PIA

IMPORTANT: PIAs that do not have sufficient information will **not** be reviewed by the OIPC. **All sections of this PIA template, whether they apply to your project or not, must be included in your submission. It is important for the OIPC to know that the public body has considered all sections of the PIA template, even though only certain sections may apply to the project under consideration. Do not modify the structure of or reformat the template, including removing any part of the template.**

Note: Consult the POPA PIA Template Completion Guide while completing the PIA.

The term "**project**" when used in this document means any information system, administrative practice, program or service, or a change to any existing information system, administrative practice, program or service a public body plans to implement that will involve the collection, use or disclosure of personal information and which includes one or more of the factors listed in section 7(5)(a) to (e) of the M-Regulation.

What a public body needs to know and have before submitting a POPA PIA to the OIPC

1. **IMPORTANT: Sections A to H of this PIA template are mandatory sections to be completed for all projects. Otherwise, the PIA will be considered incomplete and not accepted for review.**
2. **These sections are marked with an asterisk (*). The template and the PIA Completion Guide will assist you in determining how to answer the questions for your specific project.**
3. **These are mandatory requirements under POPA (referred to as "MUST" in the law) and OIPC project-specific compliance requirements.**
4. The PIA must include a cover letter signed by the ***Head of the public body*** (Appendix D).
5. Complete Appendix A if the project involves Data Matching. Otherwise indicate that this section does not apply to your project.
6. Complete Appendix B if the project is a Common or Integrated Program or Service. Otherwise indicate that this section does not apply to your project.
7. Complete Appendix C if the project includes the use of an automated system or other forms of innovative technology. Otherwise indicate that this section does not apply to your project.
8. Complete Appendix E – PIA Submission Checklist for all PIA submissions.

Please submit your PIA and the required supporting documentation to the OIPC via PIA@OIPC.AB.CA

For questions that include check boxes, click on the box (☐) to check or uncheck the box.

A. General Information About the Public Body or Bodies, Existing PIAs, and the Project *

1. Does the public body intend to collect, use or disclose personal information as part of this project?

   Personal information means recorded information about an identifiable individual. Some examples of personal information include an individual's name, home or business address, home or business email address, race, gender identity, fingerprints and financial history. For a complete listing of what is considered personal information, please see ***section 1(q) of POPA.***

   ☐Yes

   ☐No

   If yes, proceed to question 2.

   If no, there is no requirement under POPA to submit a PIA to the Commissioner for this project.

2. Does the project involve any of the following? (*The first five options are the only prescribed circumstances for which a public body is required to submit PIAs to the Commissioner under section 7(5) of the M-Regulation)*

   Select all that apply

   ☐ A practice, program, project or service will collect, use or disclose personal information deemed to be of high sensitivity *(section 1 of the M-Regulation deems biometric information about an individual, financial information about an individual, personal information respecting a minor, senior or vulnerable individual as personal information that is deemed to be of high sensitivity. See the PIA Completion Guide for more information).*

   ☐A practice, program, project or service will involve the personal information of a significant percentage of the population the public body serves.

   ☐A practice, program, project or service will involve data matching between two or more public bodies *(section 1(f) of POPA defines "data matching" as linking personal information between two or more databases or other electronic sources of information.)*

   ☐A practice, program, project or service is part of a common or integrated program or service *(section 1(d) of POPA defines "common or integrated program or service" in relation to a public body to mean a program or service planned, administered, managed, monitored or evaluated by (i) the public body working collaboratively with one or more other public bodies, or (ii) another public body working on behalf of (A) the public body, or (B) the public body and one or more other public bodies.)*

   ☐A practice, program, project or service involves the development or use of innovative technology.

   ☐None of the above (**If you select this option**, you are not required to submit a PIA to the Commissioner)

   ☐ The loss of, unauthorized access to or unauthorized disclosure of the personal information could result in significant harm.

3. Name and contact information of the public body

Provide the names and contact information for the public body participating in this PIA.

Name of public body	Name and title of head of public body	Mailing Address of public body	Email Address of head of public body	Telephone number of head of public body

4. Is this a joint PIA with any other public body?

☐Yes

☐No

If yes, complete the table below for each additional participating public body:

Public body	Name and title of head of public body	Mailing Address	Email Address	Telephone Number	Role of Public Body in this PIA

5. Contact information of the person(s) who can answer questions regarding this PIA.

This individual is responsible for communication with the OIPC during the PIA processing and review process.

Please complete the table below

Name of contact person	Role of contact person	Mailing address	Email address	Phone number

6. Name or title of the project

Every project should have a name or title for ease of reference.

7. Is this PIA related to an existing PIA that has been reviewed by the OIPC?

☐Yes
☐No

If yes, please provide the OIPC file number(s) for any related PIAs (if the file is still being processed by the OIPC, please provide the date of submission of the PIA):

8. Is this PIA an amendment to a previously submitted PIA to the OIPC?

☐Yes
☐No

If yes, please provide the OIPC file number(s) for the existing PIA(s) (if the file is still being processed by the OIPC, please provide the date of submission of the PIA):

9. Public body reference file number for this PIA (if applicable)

10. Project implementation date for the project considered for this PIA (**MM/DD/YYYY**)

11. Does this project include any of the following?
Please select all that apply.

☐Data matching –Appendix A of this PIA template must be completed.

☐Common or integrated program or service –Appendix B of this PIA template must be completed. (*A "common or integrated program or service" as described in **section 1(d) of POPA** means a program or service planned, administered, delivered, managed, monitored or evaluated by the public body working collaboratively with one or more other public bodies, **or** another public body working on behalf of the public body and one or more other public bodies.)*

☐Automated system (e.g. Artificial Intelligence) that will generate content or make decisions, recommendations or predictions; or, another form of innovative technology – Appendix C of this PIA template must be completed, including an Algorithm Impact Assessment (AIA). In addition, ensure that all relevant sections of the PIA template include information regarding the automated system and personal information that will be collected, used or disclosed by the automated system or other innovative technology.
See the POPA PIA Template Completion Guide for additional information about the purpose and details of what is required in an AIA.

☐Cloud computing - Please ensure that all relevant sections of the PIA template include information regarding any cloud computing infrastructure and service providers. In addition, both the H1 and H2 risk tables in section H of the template must be completed.

B. Details About the Project *

12. Provide a detailed description and the purpose of the project including how the collection, use and disclosure of personal information are necessary or related to this purpose or the objectives. ***(The project description should include sufficient detail including technical information about the project. Consider attaching a separate document as necessary.)***

13. Does the project involve the implementation of an electronic information system (EIS)?
An Information System is defined by the National Institute of Standards and Technology (NIST) as a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." The primary components of electronic information systems typically include hardware, software, database(s) and network(s).

☐Yes
☐No

If yes, identify the name of the system.

14. Are other stakeholders involved in the project that may collect, use or disclose personal information?

☐Yes
☐No

If yes, identify the stakeholders and describe the role of each stakeholder involved in the project, in the space provided below.
List stakeholders that may collect, use or disclose personal information associated with the project or have an impact on the privacy or security of personal information. (e.g. internal business area stakeholders; external stakeholders such as other public bodies participating in a common or integrated program or service, as well as vendors and service providers).

C. Information About Your Privacy Management Program (PMP) *

In this section, we introduce the PMP, as it may assist the public body in completing the PIA by referencing policies and procedures that may be part of the PMP. Since the PMP addresses privacy governance within the public body, the PMP contains valuable information about how the public body upholds the access and privacy rights of individuals whose personal information is collected, used or disclosed in this project.

Section 25(1) of POPA requires a public body to establish and implement a PMP and make it public or provide a copy of the PMP upon request pursuant to section 25(5). These requirements will come into effect one year after POPA came into force, which is on June 11, 2026.

15. Has the public body established and implemented a Privacy Management Program (PMP)?
    Section 6 of the M-Regulation describes what a public body must include in its PMP.

    ☐Yes
    ☐No

    If yes, **enclose a copy of the most current PMP and label it** "**Attachment - Privacy Management Program**". If you have previously submitted a PMP to the OIPC and there has been no change to it since that submission, please provide the OIPC file number for your PMP.

    If no, when will the public body finalize and implement its PMP?
    The OIPC has developed POPA PMP Guidance, which is available at https://oipc.ab.ca/popa/pmp/guide. As of June 11, 2026, section 25 will come into effect.

D. Identify Personal Information Involved and your Authority to Collect, Use or Disclose the Information*

16. List the personal information that is collected, used, or disclosed in this project and describe how the public body uses and/or discloses the information **only to the extent necessary to enable the public body** to carry out the identified purposes in a reasonable manner.

Section 12(4) of POPA requires the public body to use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner. Similarly, section 13(4) of POPA requires a public body to disclose personal information only to the extent necessary to enable the public body to carry out identified purposes in a reasonable manner. If you require additional space to list the personal information, please attach an appendix with the information.

Personal information (e.g. name, date of birth, mailing address, email, etc.)

17. Is personal information collected directly from an individual for this project?

☐Yes
☐No

If yes, provide details regarding how notice is provided to an individual at the time the personal information is collected as part of this project, pursuant to **section 5(2) of POPA**. **Also, provide a copy of the collection notice [enclose with the PIA submission and label it "Attachment 1"].**

18. Does the project use or disclose any personal information with the consent of the individual pursuant to section 12(1)(b) or section 13(1)(c) of POPA, and the requirements of section 2 of the Protection of Privacy Regulation (the Regulation)?

☐Yes
☐No

If yes:

- **Provide a copy of the policy and procedure(s) that address consent [enclose with the PIA submission and label it "Attachment 2"]. OR if you have provided this information to our office as part of your PMP, identify the policy and procedure(s) that address consent in your PMP submission.**

- **Provide a copy of the consent form for use and disclosure of personal information involved in the project [enclose with the PIA submission and label it "Attachment 3"].**

19. Will any personal information about an individual be collected indirectly?

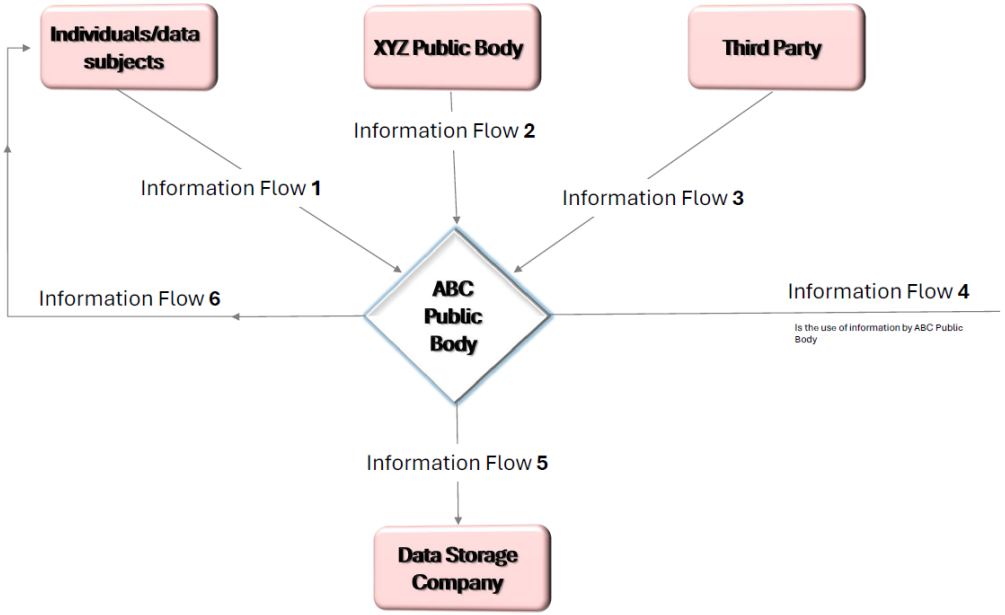
☐Yes
☐No

If yes, explain **how** personal information will be collected indirectly. Ensure you identify the data flow in the information flow diagram and legal authority table below.

20. Information flow diagram

An information flow diagram illustrates how personal information is collected, used or disclosed in this project. It identifies the various stakeholders and systems associated with the collection, use or disclosure of personal information. The diagram should clearly label each flow with a number, the direction that information is flowing as well as to whom the information is flowing. Note that a project, depending on its complexity, may have more than one information flow diagram. ***Note that a business process flow or network diagram is not an information flow diagram. For additional information regarding the differences between a network, process flow and data flow diagram, please see the POPA PIA Template Completion Guide.***

See the following information flow diagram example.



Attach a copy of the information flow diagram(s) for this project [enclose with the PIA submission and label it "Attachment 4"].
Note: If an information flow diagram is not attached, the PIA will be deemed incomplete and will not be reviewed.

21. Using the table below, identify and describe the legal authorities and purposes for the collection, method of collection (direct or indirect), use or disclosure of personal information in this project.

    A public body is prohibited from collecting (directly or indirectly), using or disclosing personal information except as permitted by sections 4, 12, and 13 of POPA.

    Identify each information flow number in your information flow diagram(s) and include the corresponding description of the information in the table below.

Information Flow #	Description of Information Flow (if the flow is a collection, indicate whether it is direct or indirect collection) *Explain how the information flows between parties, systems, etc.*	Personal Information Involved	Stakeholder Involved in the Collection (direct or indirect), Use and/or Disclosure of personal information	Purpose for Collection, Use and/or Disclosure	Legal Authority for Collection (direct or indirect), Use or Disclosure (cite specific sections of POPA and any other relevant legislation)
Example flow 1	ABC public body collects personal information directly from the individuals the information is about.	First name, last name, mailing address, email address	ABC public body and individuals	This information is collected from individuals to enroll them into the program provided by ABC public body.	POPA s. 4(c)
1					
2					
3					
4					
5					
6					

E. Access, Correction, Accuracy, Retention, Disposition *

For the questions that ask you to describe certain processes (e.g. describe how an individual can request access to their personal information), ensure the answer to the question includes a fulsome description of the process, rather than limiting the response to a policy name or reference. In addition, explain how the policy referenced applies to the project.

22. Describe how individuals are made aware of their right to access their personal information that is involved in this project and how they can exercise that right.

Section 6 of the Access to Information Act (ATIA) *provides individuals with a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the individuals. Additionally, the right of access enables individuals to know what the public body holds about them in order to assess accuracy or request correction.*

23. Does the public body have an access request policy?

☐Yes

☐No

If yes, and if the public body has provided this information to our office as part of its latest PMP submission, identify the policy and procedure that address access requests in the public body's PMP submission, below; otherwise, provide a copy of the policy and procedure(s) that address access requests **[enclose with the PIA submission and label it "Attachment 5**"].

If no, describe the steps that you are taking to develop and implement such a policy and provide a timeline by which the policy will be in place.

24. Describe how individuals are made aware of their right to request correction of their personal information that is involved in this project and how they can exercise that right.

Section 7 of POPA *provides an individual with the right to request the head of the public body that has the information in its custody or under its control to correct their personal information, if the individual believes there is an error or omission in the individual's personal information.*

25. Does the public body have a correction request policy?

☐Yes
☐No

If yes, and if the public body has provided this information to our office as part of its current PMP submission, identify the policy and procedure that address correction requests in the public body's PMP submission, below; otherwise, provide a copy of the policy and procedure(s) that address correction requests **[enclose with the PIA submission and label it "Attachment 6"]**

If no, describe the steps that you are taking to develop and implement such a policy and provide a timeline by which the policy will be in place.

26. Describe how the public body will ensure that the personal information involved in this project will be accurate and complete?

Section 6 of POPA *requires the public body to make every reasonable effort to ensure personal information that will be used by a public body to make a decision that directly affects an individual is accurate and complete. Examples of methods that public bodies may use to ensure personal information is accurate and complete are as follows:*

- *Training and awareness for employees who perform data entry into systems.*
- *Policies and procedures that govern and describe the activities associated with the integrity of personal information.*
- *Configuration of input controls within information systems that ensure correct inputs are accepted by the systems.*
- *Configuration of access controls within information systems that restrict the activities that users may perform on personal information, based on job requirements.*
- *Capturing and reviewing audit logs of activities in a system to detect and address data integrity issues.*
- *Implementing IT change management practices that align with industry standards for changes to information systems.*

27. Has the public body established and implemented a record retention and disposition policy for personal information involved in this project? ***Section 6 (b) of POPA*** *requires that personal information used to make a decision that directly affects an individual be retained for at least one year to enable the individual who is the subject of the information to obtain access to the information, or for a shorter period if agreed to in writing by the individual, the public body, and, as applicable, another body that may be involved in records retention.*

☐Yes
☐No

If yes, and if the public body has provided this information to our office as part of its current PMP submission, identify the policy and procedure that address record retention and disposition for this project in the PMP submission, below; otherwise, provide a copy of the policy and procedure(s) that address record retention and disposition **[enclose with the PIA submission and label it "Attachment 7"]**.

If no, describe the steps that you are taking to develop and implement such a policy and provide a timeline by which the policy will be in place.

28. if you answered "**yes"** to question 27 and if the project involves the use of an electronic information system to process personal information, describe the steps that the public body has taken to implement the record retention and disposition policy in the electronic information system *(considerations in your response should include but are not limited to indicating whether someone has been assigned the responsibility for the public body's record retention and disposition practices, associated policy and processes as well as describing measures that are in place to demonstrate that the public body is adhering to the policy.)*

F. Protection of Information *

Section 10(1) of POPA *requires the head of a public body to protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.* ***Section 1(1)(c) of the Regulation*** *defines "reasonable security arrangements" as administrative safeguards, physical safeguards and technical safeguards to protect personal information, data derived from personal information and non-personal data in the custody or under the control of a public body that are appropriate and proportional to the security classification level of the information or data, and in the case of non-personal data, ensure, to the extent possible, that the identity of an individual who is the subject of the non-personal data cannot be re-identified from the data. In addition, the* ***M-Regulation*** *sets out additional requirements for the security classification of personal information.*

Information about protecting the personal information involved in the project

29. Has the public body assigned a security classification to the personal information involved in the project?
    Section 2(1) of the M-Regulation *requires a public body to assign a security classification level to all personal information, data derived from personal information and non-personal data in the custody or under the control of the public body, based on an internal classification system established by the public body.* ***Section 2(2) of the M-Regulation*** *requires the security classification level assigned to personal information to reflect the sensitivity of the personal information.* ***Note: This is a HARD REQUIREMENT. PIA submissions that do not include information regarding the public body's information security classification system will not be reviewed.***

    ☐Yes
    ☐No

    If yes, identify and describe the classification level of the information in relation to the public body's information classification system.

    If no, the public body must assign a security classification to the personal information involved in the project prior to submitting this PIA.

30. Using the boxes below, describe how the public body will ensure that the personal information involved in this project is protected against such risks as unauthorized access, collection, use, disclosure or destruction **that are appropriate and proportional to the classification of the personal information**.
Note: This is a HARD REQUIREMENT. PIA submissions that do not include information regarding the public body's safeguards will not be reviewed.

If the project involves a high volume of personal information or highly sensitive personal information, policies and procedures must be documented and attached to this PIA submission as required by section 6(2) of the M-Regulation **[enclose with the PIA submission and label it "Protection of Personal Information Policies and Procedures"]**.
If the policies have been included as part of a PMP submission included in this PIA, include the policy reference (i.e. policy name and page number). However, note that reference to general policies and procedures alone will not be sufficient. Details about how the policies and procedures contribute to the safeguarding of personal information involved **in this project** must also be provided.

a. Describe the administrative safeguards in place to protect the information involved in the project.
Section 1(2)(a) of the Regulation *describes an "administrative safeguard" as a policy, procedure or practice to manage a public body's conduct that protects the privacy of personal information, data derived from personal information and non-personal data.*
(Some examples of administrative safeguards include documented policies and procedures, security and privacy awareness training, confidentiality agreements, contracts and agreements.)

b. Describe the physical safeguards in place to protect the information involved in the project.
Section 1(2)(b) of the Regulation *describes a "physical safeguard" as a method to protect a public body's physical assets, including electronic information systems, from natural and environmental hazards and unauthorized intrusion.*
(Some examples of physical safeguards include locked filing cabinets, alarms on premises, locked server rooms, personal information stored out of reach of the public, temperature monitoring and response system, humidity monitoring and response system, fire detection and suppression systems).

c. Describe the technical safeguards in place to protect the information involved in the project.
Section 1(2)(c) of the Regulation *describes a "technical safeguard" as a method to protect a public body's electronic data and access to it.*
(Some examples of technical safeguards include network security controls, application security controls, systems access controls, etc.)

31. Describe how the public body continuously assesses and monitors the safeguards described in the above question to ensure they are working as expected to protect personal information.

32. As it relates to this project, does the public body have a process to ensure its employees are aware of their duty to notify the head of the public body of any loss of, unauthorized access to, or unauthorized disclosure of personal information (**Section 10(2) of POPA**)?

☐Yes
☐No

If yes, describe how the public body makes its employees aware of their duty to notify the head of the public body of any loss of, unauthorized access to or unauthorized disclosure of personal information (*considerations should include sections of the public body's policies and processes as well as training that ensure employees are aware of the actions to take*).

If no, describe the steps the public body will take to make its employees aware of their duty to notify the head of the public body of any loss of, unauthorized access to or unauthorized disclosure of personal information involved in this project, and provide a timeline by which this will be done.

Protection of personal information in information systems

Complete this section if the project involves the implementation of an Electronic Information System (EIS).

33. Does the public body have an access control policy and associated procedure(s) that relate to access to personal information in the EIS?
Note: If the public body is implementing an EIS that processes a high volume of personal information or highly sensitive personal information, this is a HARD REQUIREMENT. PIA submissions that do not include information regarding the public body's access control policy will not be reviewed.

If the project involves a high volume of personal information or highly sensitive personal information, a documented access control policy must also be attached to this PIA submission (see section 6(2) of the M-Regulation)

☐Yes
☐No

If yes, and if the public body has provided this information to our office as part of its current PMP submission, identify the policy and procedure that address access to personal information in the EIS in the public body's PMP submission, below; otherwise, provide a copy of the policy and procedure(s) that address access to the personal information in the EIS **[enclose with the PIA submission and label it "Attachment 8"]**.

If no, and the project involves a high volume of personal information or highly sensitive personal information, the public body must develop and document an access control policy prior to submitting this PIA. ***(see section 6(2) of the M-Regulation)***

If no, and the project ***does not*** involve a high volume of personal information or highly sensitive personal information, proceed to question 34.

34. Describe the process for approving access to personal information within the information system.

35. Provide details regarding how access is limited to only those employees who have a defined business requirement to access personal information and how their access is limited to only the amount of information required to perform their job duties.

36. Describe the process for revoking access to the information system in a timely manner when such access is no longer required (e.g. employee changes role or employee leaves the organization).

37. Complete the access table, below:

Position or job title	System user role	Number of staff in this role	Permissions assigned to the role (create, read, write, modify, delete, execute, etc.)	Description of information this user can access and description of the actions the user can take (include examples)
(E.g. School Clerk)	(E.g. Admin Support)	(e.g. 2)	(E.g. read, write, modify)	(E.g. school administrative support staff can only view and modify registration information but has no access to student grades)

Logging and Auditing Access to the EIS

38. Does the public body have a logging and auditing policy and associated procedure(s) for this EIS?

Note: If the public body is implementing an EIS that processes a high volume or highly sensitive personal information, this is a HARD REQUIREMENT. PIA submissions that do not include information regarding the public body's access control policy will not be reviewed.

****If the project involves a high volume of personal information or highly sensitive personal information, a documented logging and auditing policy must be attached to this PIA submission*. (section 6(2) of M-Regulation)**

☐Yes
☐No

If yes, and if the public body has provided this information to our office as part of its current PMP submission, identify the policy and procedure that address logging and auditing in the public body's PMP submission, below. Otherwise, provide a copy of the policy and procedure(s) that address logging and auditing **[enclose with the PIA submission and label it "Attachment 9"]**.

If no, and the project involves a high volume of personal information or highly sensitive personal information, the public body must develop and document a logging and auditing policy prior to submitting this PIA.

If no, and the project ***does not*** involve a high volume of personal information or highly sensitive personal information, describe the process (or if you have documentation include it) by which the public body logs and audits activities associated with access to personal information stored in the EIS.

39. Does the system capture and maintain audit logs of access to personal information?

☐Yes
☐No

If yes, use the table below to identify the data elements that are captured in the information system's audit logs.

Audit log data elements	Description	Comments (if applicable)
(E.g. user ID)	(E.g. uniquely identifies a user of the system)	

Audit log data elements	Description	Comments (if applicable)

If no, describe the steps the public body will take to ensure the system captures and maintains audit logs of access to personal information and provide a timeline by which this will be done.

40. Describe the steps taken by the public body to proactively audit access to personal information in the information system.

41. Provide information regarding the audit criteria, the frequency of audits and who conducts the audits.

A public body may consider several factors in determining the frequency to conduct audits, such as the number of users who have access to information in the system, the volume and sensitivity of personal information. Some examples of audit report criteria include, but are not limited to, users accessing the personal information of individuals with the same last name and same physical address, frequently accessed records, frequently failed login attempts, and inactivity audits.

G. Service Providers *

Section 1(h) of POPA *states that an "employee" in relation to a public body, includes "a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body". As the public body is ultimately accountable for the actions of its employees in relation to its compliance with POPA, it is important for the public body to enter into contracts or agreements with any third parties that provide services to the*

public body to ensure each third party complies with POPA. In this section, you will identify the third parties of the public body, the contracts or agreements that are in place and the responsibilities of the third parties regarding privacy and security of personal information. "Person" is defined in the Interpretation Act, section 28(1)(nn) to include a corporation.

42. Does the public body use service providers, including vendors and contractors, in this project that will have access to personal information or will collect, use or disclose personal information on its behalf? (*The public body must ensure that personal information collected, used or disclosed by the service provider is captured in the information flow diagram and corresponding legal authority table in section D of this PIA.*)

☐Yes
☐No

If yes, proceed and use the table below to provide additional information about the nature of the relationship.
If no, proceed to Section H of the template.

Name of third party	**Relationship with the Public Body**	**Description of services provided**	**Type of agreement or contract that establishes a service provider relationship with public body** *(Documents referenced below must be provided as part of the PIA submission.)*
(E.g. ABC Web Services)	(E.g. Service Provider)	(e.g. web hosting)	(E.g. service agreement)

43. For this project, does the public body have a contractual agreement with its service provider that addresses its duties under POPA as it relates to the service of the service provider, and the privacy and security of personal information under POPA?
Pursuant to section 1(h) of POPA, employee", in relation to a public body, includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body. This means that a service provider may considered an employee of the public body and must comply with POPA.
Note: If the public body engages the services of third-party service providers, this is a HARD REQUIREMENT. PIA submissions that do not indicate that there is a contract or agreement in place with third-party service providers will not be reviewed.

☐Yes
☐No

If yes, proceed to the next question.

If no, the public body must ensure it has a contractual agreement(s) with its service provider(s) that addresses all its compliance obligations under POPA that will be imposed on the service provider to ensure compliance before submitting the PIA.

44. For this project, will the service provider process access to information requests on behalf of the public body?

☐Yes
☐No

If yes, describe the steps that the public body has taken to ensure the contractual agreement with the service provider addresses access to information request processing.

If no, proceed to the next question.

45. For this project, has the public body clarified in its contractual agreement(s) with the service provider(s), that the public body maintains control of any information that the service provider(s) accesses, collects or uses in relation to the services which the service provider(s) provides to the public body?
Note: If the public body engages the services of third-party service providers, this is a <u>HARD REQUIREMENT</u>. PIA submissions that do not include a copy of associated contracts or agreements will not be reviewed.

☐Yes
☐No

If yes, provide a copy of the agreement(s) and identify the provisions in the agreement that ensure the public body maintains control of the information. **[enclose with the PIA submission and label it "Attachment 10"]**.

If no, the public body must ensure it has a contractual agreement(s) with its service provider that ensures the public body maintains control of information involved with the project before it submits its PIA.

46. Does the contractual agreement(s) in place with the public body's service provider(s) identify each party's responsibilities related to the privacy and security of personal information?

☐Yes
☐No

If **yes**, identify the sections of the agreement(s) that describe the privacy and security provisions, including any provisions that pertain to the collection, use, disclosure, protection, retention of personal information and termination provisions.

If no, describe the steps the public body will take to meet these requirements and the timeframe by which the public body will meet these requirements.

47. Identify sections of the contractual agreement(s) with the service provider(s) that address(es) ongoing training requirements for the employees of the service provider(s) who have access to personal information involved in this project.

H. Project Risk Assessment and Mitigation *

Complete the following privacy risk assessment and mitigation table for this project. The risks listed under the section are common privacy risks that may exist in projects. The public body is responsible for identifying all other risks that may exist in this project.

48. Did the public body conduct a security threat and risk assessment (STRA), including a vulnerability assessment (VA) and penetration test (pentest) for the project?

☐Yes
☐No
☐N/A

If yes, attach copies of the STRA reports including VA and pentest reports and the steps that the public body has taken to address identified security issues **[enclose with the PIA submission and label it "Attachment 11"]**.

If no or N/A, provide clarification as to why a STRA including VA and pentest was not completed or deemed necessary for the project.

H1. General Risks (to be completed for all PIA submissions) *

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Unauthorized collection of personal information by authorized users (e.g. an employee, contractor, vendor, etc.) contrary to section 4 and 5 of POPA	E.g. personal information is collected by the public body and/or the information system is configured to accept personal information that does not relate directly to and is not necessary for the project.		
2.	Unauthorized use of personal information by authorized users			
3.	Unauthorized disclosure of personal information by authorized users.			
4.	Unauthorized access to personal information by unauthorized users or malicious software (e.g. ransomware)			
5.	Loss of personal information			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
6.	Loss of custody or control of personal information			
7.	Unauthorized destruction of personal information			
8.	Loss of integrity including unauthorized modification of personal information.			
9.	Unauthorized retention of personal information.			
10.	Lack of notice or proper notice at the time of collection of personal information collected for this project.			
11.	Lack of clarity or failure to provide information regarding access to or correction of information.			
12.	Lack of or inadequate privacy breach management policies and procedures.			
13.	Lack of assessment by the public body of third parties' (e.g. service providers) privacy and security controls regarding the management of personal information on behalf of the public body			
14.	Use or disclosure of personal information for secondary purposes by the public body or its service providers without proper authority.			
15.	Logging and auditing controls of personal information are insufficient or absent, contrary to section 3(2) of the M-Regulation.			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
16.	Lack of human oversight and validation measures for systems, contrary to section 3(2) of the M-Regulation.			
17.	Failure to conduct a vulnerability assessment to identify and address exploitable security vulnerabilities associated with the implemented system.			
18.	Insert additional risks identified by the public body			

H2. Risks Associated with Cloud Computing

☐**N/A (check this if it does not apply)**

Complete this section if the public body is using or intends to use a cloud computing provider to store or manage personal information as part of this project.

Risk number	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Inadequate segregation and isolation of the public body's cloud environment containing personal information from the cloud provider's other customers in a multi-tenant environment.	E.g., in multitenant cloud environment compromise of one environment could lead to the compromise of other environments due to inappropriate segregation and isolation. In addition, there could potentially be information leakage between environments leading to unauthorize disclosure of personal information.		

Risk number	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
2.	Contracts or agreements are either not in place with the cloud provider or are insufficient.			
3.	The cloud provider does not have a robust privacy and security governance structure.			
4.	Lack of clarity regarding the cloud provider's responsibility to notify the public body of the breach in a timely manner.			
5.	Vendor or cloud provider lock-out.			
6.	Vendor or cloud provider lock-in.			
7.	Unauthorized access to personal information by foreign governments or states.			
8.	The cloud provider uses personal information for purposes not authorized by POPA.			
9.	The cloud provider discloses personal information for purposes not authorized by POPA.			
10.	Broken authentication and authorization.			

Risk number	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
11.	Use of weak cryptographic algorithms or lack of encryption of data in transit and at rest.			
12.	Insert additional risks identified by the public body.			

H3. Risks Associated with Research

☐N/A (check this if it does not apply)

Complete this section if the public body intends to disclose personal information for research or statistical purposes as part of this project.

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Disclosure of personal information for research or statistical purposes is contrary to section 15(a) of POPA.	E.g. the public body fails to assess whether non-identifying data can be used to accomplish the research purpose prior to disclosing individually identifying personal information [s.15(a)(i) of POPA] or the research purpose has not been approved by Commissioner [15(a)(ii) of POPA].		
2.	Disclosure of personal information for research or statistical purposes that is not clearly in the public interest, contrary to section 15(b) of POPA.			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
3.	Disclosure of personal information for research or statistical purposes that may be harmful to an individual, contrary to section 15(b) of POPA.			
4.	Disclosure of personal information for research or statistical purposes contrary to section 15(c) of POPA.			
5.	Lack of or insufficient research agreement contrary to section 15(d) of POPA and section 4 of the Protection of Privacy Regulation.			
6.	Insert additional risks identified by the public body			

Appendix A. Data Matching

Data matching *means linking personal information between 2 or more databases or other electronic sources of information (section 1(f) of POPA). In this section, you will address the public body's intent to carry out data matching and assess whether the public body meets its obligations under POPA related to data matching.*

1. Is the public body carrying out data matching with another public body?
   ☐Yes
   ☐No

   If yes, complete the rest of Appendix A.
   If no, the public body does not need to complete the rest of Appendix A.

2. What is the purpose(s) for the data matching?
Section 17(1) of POPA *authorizes a public body to carry out data matching to create data derived from personal information only for specific purposes.*

Select all that apply.

☐Research and analysis

☐Planning, administering, delivering, managing, monitoring or evaluating a program or services

☐ One or more prescribed purposes.

3. How does the public body obtain personal information to be used for data matching?
Section 17(3) of POPA *prohibits public bodies from collecting personal information directly from an individual when the collection is for the purposes of data matching; however, the public body may collect personal information from another public body or use personal information in its custody or under its control for data matching purposes.*

Select all that apply

☐Collecting from another public body (proceed to question 4 if this is selected)

☐Using personal information in the public body's custody or control (if this is the only option that is selected, proceed to question 7)

4. If the public body is collecting personal information from another public body for the purpose of carrying out data matching, has the public body established a clear governance structure respecting the responsibilities and accountability of each public body involved in the collection of personal information for the purpose of carrying out data matching?
Section 7(2)(g) of the M-Regulation *requires a public body to establish a clear governance structure if a public body is collecting personal information from another public body under* ***section 17(3) of POPA*** *for the purposes of data matching.*
Note: This is a HARD REQUIREMENT. PIA submissions that do not include documentation of the governance structure will not be reviewed.
Note: The governance structure should, at minimum, contain certain requirements as listed in the POPA PIA Template Completion Guide

☐Yes

☐No

If yes, attach documentation related to the governance structure **[enclose with the PIA submission and label it "Attachment 12"]**.

If no, the public body must implement a clear governance structure that meets the requirements of the M-Regulation prior to submitting the PIA.

5. If the public body is collecting personal information from another public body under section 17(3) of POPA for the purpose of data matching, has the public body entered into an agreement with the other public body from which the public body intends to collect personal information?

   Note: This is a HARD REQUIREMENT. PIA submissions that do not include a copy of the agreement will not be reviewed.
   Note: The agreement should, at minimum, contain certain requirements as listed in the POPA PIA Template Completion Guide. Public bodies must meet these requirements before submitting their PIAs to the Commissioner for review.

   ☐Yes
   ☐No

   If yes, attach a copy of the agreement **[enclose with the PIA submission and label it "Attachment 13"]** and identify the sections of the agreement that address the requirements listed in the **POPA PIA Template Completion Guide**.

   If no, the public body must enter into an agreement with the other public body prior to submitting this PIA.

6. For the data matching, is the public body submitting this PIA performing any unique collection, use or disclosure of information that only applies to the public body?

   Section 7(4)(b) of the M-Regulation *authorizes a public body to prepare a joint PIA to describe the data matching, but requires each participating public body to, in addition to the joint PIA, prepare an addendum to address any unique collection, use or disclosure circumstances that apply to that public body.*
   Note: If the public body is performing any unique collection, use or disclosure that only applies to the public body, this is a HARD REQUIREMENT. PIA submissions that do not include a copy of the PIA addendum will not be reviewed.

   ☐Yes
   ☐No

   If yes, attach a copy of the addendum **[enclose with the PIA submission and label it "Attachment 14"]**

The public body must prepare an addendum for data matching that meets the requirements of section 7(4)(b) of the M-Regulation and must include the addendum when submitting a joint PIA.

If no, proceed to the next question.

7. Describe the security arrangements that are in place to protect personal information associated with data matching.
Section 17(2) of POPA *requires the public body to carry out data matching in accordance with the prescribed security arrangements in accordance with* ***section 3(1) of the M-Regulation****.* ***Section 3(1) of the M-Regulation*** *requires public bodies to implement reasonable administrative, physical and technical safeguards to protect personal information against such risks as unauthorized access, collection, use, disclosure or destruction. The security arrangements must be appropriate and proportional with the security classification level of that information or data.*
If the security arrangements that have been described elsewhere also apply to the safeguarding of personal information associated with data matching, indicate where in this PIA template and the public body's policy documents this information is captured.

8. Please complete the following Risk Assessment and Mitigation table for risks related to Data Matching

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Failure to establish a clear governance structure respecting the responsibilities and accountability of the public body conducting the data matching and those of the public body from which personal information is collected for the purpose of data matching, if personal information is collected from another public body for the purpose of data matching.	e.g. section 7(2)(g) of the M-Regulation requires the establishment of a clear governance structure respecting the responsibilities and accountability of two public bodies involved in data matching if one public body is collecting personal information for another public body for the purpose of data matching.		

2.	Collection of personal information directly from individuals for the purpose of data matching contrary to section 17(3) of POPA.			
3.	The data matching process or method is not well defined and properly implemented leading to errors in the resulting data.			
4.	Data quality of the source data used for data matching are not adequately assessed and validated leading to data integrity issues in the resulting data.			
5.	Failure to implement reasonable security controls within the data matching environment thereby exposing personal information to potential loss unauthorized access or unauthorized disclosure.			
6.	Failure to establish and implement a data validation or test process to ensure the resulting data set from the data matching process is the desired and accurate outcome.			
7.	Failure to securely remove personal information from the data matching environment upon completion for the data matching process thereby exposing personal information to potential unauthorized access.			
8.	Insert additional risks identified by the public body.			

Appendix B. Common or Integrated Program or Service

*A "common or integrated program or service" pursuant to **section 1(d) of POPA** means a program or service planned, administered, delivered, managed, monitored or evaluated by the public body working collaboratively with one or more other public bodies, **or** another public body working on behalf of the public body and one or more other public bodies.*

1. Is the project a common or integrated program or service?

   ☐Yes
   ☐No

   If yes, complete the rest of Appendix B.
   If no, the public body does not need to complete the rest of Appendix B.

2. Is this a new common or integrated program or service or a change to an existing common or integrated program or service?

   ☐A new common or integrated program or service
   ☐A change to an existing common or integrated program or service

   a. List the other public body or public bodies with which the public body submitting this PIA is collaborating or for which the public body submitting this PIA is working on behalf of for the purposes of the common or integrated program or service.

   b. If this is a joint PIA submission, identify the public body coordinating the submission of this PIA on behalf of the other public body or public bodies?

c. If this is a change to an existing common or integrated program or service, provide the **OIPC PIA file number** for the existing PIA or identify the date the existing PIA was submitted to the OIPC if it is still being processed by the OIPC and the file number has not yet been issued for the PIA.

3. Has the public body, engaging in a common or integrated program or service with one or more other public bodies, established a clear governance structure respecting the responsibilities and accountability of each public body involved in the common or integrated program or service?

   Section 7(2)(g) of the M-Regulation *requires the public body to have a clear governance structure respecting the responsibilities and accountability of each public body if two or more public bodies are engaging in a common or integrated program or service.*

   A governance structure is a documented set of rules and processes that identify the roles, responsibilities, and accountability of each public body participating in the integrated program or service.

   Note: This is a HARD REQUIREMENT. PIA submissions that do not include documentation of the governance structure will not be reviewed.

   Note: The governance structure should, at minimum, contain certain requirements as listed in the POPA PIA Template Completion Guide

   ☐Yes
   ☐No

   If yes, attach documentation related to the governance structure **[enclose with the PIA submission and label it "Attachment 15"]**.

   If no, the public body must implement a clear and documented governance structure that meets the requirements of Section 7(2)(g) of the M-Regulation prior to submitting the PIA. The governance structure must have been implemented if the project has been launched or be implemented prior to launching the project if the project is yet to be launched.

4. Has the public body engaged in a common or integrated program or service with one or more other public bodies, entered into an agreement with the other public body or public bodies that addresses how each public body involved in the common or integrated program or service complies with POPA?

   Note: This is a HARD REQUIREMENT. PIA submissions that do not include a copy of the agreement will not be reviewed.

   Note: The agreement should, at minimum, contain certain requirements as listed in the POPA PIA Template Completion Guide Public bodies must meet these requirements before submitting their PIAs to the Commissioner for review.

☐Yes
☐No

If yes, attach a copy of the agreement **[enclose with the PIA submission and label it "Attachment 16"]** and identify the sections of the agreement that address the requirements listed in the **POPA PIA Template Completion Guide**.

If no, the public body must enter into an agreement with the other public body or public bodies prior to submitting this PIA.

5. For the common or integrated program or service, is the public body submitting this PIA performing any unique collection, use or disclosure of information that only applies to the public body?

Section 7(4)(b) of the M-Regulation *authorizes a public body to prepare a joint PIA to describe a common or integrated program or service, but requires each participating public body to, in addition to the joint PIA, prepare an addendum to address any unique collection, use or disclosure circumstances that apply to that public body.*

Note: If the public body is performing any unique collection, use or disclosure that only applies to the public body, this is a* HARD REQUIREMENT*. PIA submissions that do not include a copy of the PIA addendum will not be reviewed.

☐Yes
☐No

If yes, attach a copy of the addendum **[enclose with the PIA submission and label it "Attachment 17"]**.

The public body must prepare an addendum for any unique collection, use or disclosure applicable to the public body that meets the requirements of section 7(4)(b) of the M-Regulation. The addendum must be included with the PIA submission.

6. Please complete the following Risk Assessment and Mitigation table for risks related to common or integrated programs or services.

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Lack of clear governance for common or integrated program or service contrary to section 7(2)(g) of the M-Regulation.	E.g. governance structure including policies are not in place or are inadequate leading to inconsistencies in the management of the program that creates exploitable privacy and security vulnerabilities.		
2.	Lack of clarity in accountability for different aspects of the program or service.			
3.	Lack of clarity in responsibility for different aspects of the program or service.			
4.	Lack of alignment between the public body's Privacy Management Program and the governance structure of the common or integrated program or service.			
5.	Lack of transparency regarding how individuals' access and privacy rights are upheld.			
6.	Insert additional risks identified by the public body.			

Appendix C. Use of Automated Systems or Other Forms of Innovative Technology

☐**N/A (check if this does not apply)**

Complete this section if the public body intends to use an automated system, such as Artificial Intelligence (AI) or other forms of innovative technology that generates content or makes decisions, recommendations.

1. Has the public body completed an Algorithmic Impact Assessment (AIA) for this project?
   See the POPA PIA Template Completion Guide for additional information about the purpose and details of what is required in an AIA.

   ☐Yes
   ☐No

   If yes, **attach a copy of the AIA for this project [enclose with the PIA submission and label it "Attachment 18"]**.

2. Please complete the following Risk Assessment and Mitigation table for risks related to automated systems (e.g. AI) or other forms of innovative technology.

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Loss of custody or control of personal information in an automated system that is hosted by a third party.	E.g. failure to maintain custody or control of personal information ingested by an AI system due to lack of controls to securely and automatically delete information from the AI system.		
2.	Lack of or insufficient policies and procedures to govern automated systems or other innovative technology implementation.			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
3.	Lack of clarity on processes and tools in place to ensure accuracy in an automated system's decision making.			
4.	Lack of clarify on how the quality and reliability of an automated system model training data to minimize bias and inaccurate automated decisions including hallucination.			
5.	Automated system inputs are not validated and securely protected, making the inputs vulnerable to tempering.			
6.	Lack of understanding of what automated system training model (static or dynamic) is implemented and how the model is monitored and kept up to date to ensure it works within its defined parameters.			
7.	The automated system model is not well adjusted to the training data (underfitting) leading to broad generalization and inaccurate results (false positives) with new data.			
8.	The automated system model is too adjusted to the training data (overfitting) leading to lack of generalization and possible inaccurate or unsatisfactory results using new data results (false negatives).			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
9.	The automated system is not securely configured, making it vulnerable to compromise.			
10.	Lack of processes for individuals to be made aware of and appeal automated decisions made by automated systems.			
11.	Insufficient logging and auditing controls associated with the automated system or the innovative technology.			
12.	Lack of monitoring of the automated system or other innovative technology system to ensure it is functioning as intended.			
13.	Failure to conduct security vulnerability on the automated system or other innovative technology system to identify and address exploitable security weaknesses.			
14.	Additional risks identified by the public body related to automated systems and/or other forms of innovative technology.			

Appendix D. PIA Cover Letter *

PIA COVER LETTER WORDING

(Customize the areas highlighted in yellow and attach the cover letter on public body official letterhead)

Submitted electronically

DATE

Information and Privacy Commissioner
Suite 410, 9925-109 Street NW
Edmonton, AB T5K 2J8

Dear {INSERT NAME OF THE INFORMATION AND PRIVACY COMMISSIONER}:

Re: {INSERT TITLE OF PROJECT} – {INSERT PUBLIC BODY FILE #, IF APPLICABLE}

Please find attached our privacy impact assessment (PIA) for the above-named project. I am making this submission in accordance with section 26(1) of the *Protection of Privacy Act* (POPA).

The PIA is current as of this submission to your office. I understand that as things change in our project, I will update the PIA by highlighting the sections that have changed, assessing the privacy impact of the change and submit an updated version to your office. If there are substantive changes, I will submit a new PIA to your office which will replace any initial submission(s).

Sincerely,

{SIGNATURE OF THE HEAD OF THE PUBLIC BODY}

{INSERT NAME AND TITLE OF HEAD (OR DESIGNATRE) OF PUBLIC BODY AND NAME OF THE PUBLIC BODY}

C:

Appendix E. PIA Submission Checklist *

Detailed Requirements of the PIA – Mandatory Section of the PIA	
Indicate whether you have completed the following sections of the PIA template. Any sections identified with an asterisk (*) are mandatory.	
Mandatory Section of the PIA Template	**Is the section completed and included?**
Cover Letter (Appendix D) *	☐Yes
Section A *- General Information about the public body or bodies, existing PIAs, and the project	☐Yes
Section B * - Details About the Project	☐Yes
Section C * - Information About Your Privacy Management Program (PMP)	☐Yes
Section D * - Identify Personal Information Involved and Collection, Use or Disclosure Authority	☐Yes
Section E * - Access, Correction, Accuracy, Retention, Disposition	☐Yes
Section F * - Protection of Information	☐Yes
Section G * - Service Providers	☐Yes
Section H * - Project Risk Assessment and Mitigation	☐Yes

Detailed Requirements of the PIA – Project-Dependent Sections of the PIA	
Indicate whether you have completed the following sections of the PIA template.	
Project-Specific Section of the PIA Template	**Has the public body considered and completed the following sections?**
Appendix A – Data Matching	☐Yes - completed and included ☐N/A - not completed but considered.
Appendix B – Common or Integrated Program or Service	☐Yes - completed and included ☐N/A - not completed but considered.
Appendix C – Use of Automated Systems or other Forms of Innovative Technology	☐Yes - completed and included ☐N/A - not completed but considered.

Attachments to be enclosed with the PIA	
Indicate whether you have attached the requested attachments (where required) for the project. Any attachments identified with an asterisk (*) are required to be included with your PIA submission.	
Attachment	**Has the public body completed and enclosed the following attachments?**
Privacy Management Program (PMP)	☐Yes ☐No
Protection of Personal Information Policies and Procedures	☐Yes ☐No ☐Included in enclosed PMP
Attachment 1* – Collection Notice	☐Yes ☐Included in enclosed PMP
Attachment 2*- Consent Practices (Policies and Procedures)	☐Yes ☐Included in enclosed PMP
Attachment 3*- Consent Form	☐Yes ☐Included in enclosed PMP
Attachment 4* - Information Flow Diagram	☐Yes ☐Included in enclosed PMP
Attachment 5 - Request to Access Personal Information Practices (Policies and Procedures)	☐Yes ☐No ☐Included in enclosed PMP
Attachment 6 - Correction of Personal Information Request Practices (Policies and Procedures)	☐Yes ☐No ☐Included in enclosed PMP
Attachment 7- Record Retention and Disposition Practices (Policies, Procedures, Retention Schedule)	☐Yes ☐No ☐Included in enclosed PMP

Attachment	Has the public body completed and enclosed the following attachments?
Attachment 8 *- Access to Personal Information in EIS Practices (Policies and Procedures) (required where applicable)	☐Yes ☐N/A ☐Included in enclosed PMP
Attachment 9 * – Audit and Logging of Personal Information in EIS (Policies and Procedures) (required where applicable)	☐Yes ☐N/A ☐Included in enclosed PMP
Attachment 10 * – Contracts and Agreements with Third Parties (required where applicable)	☐Yes ☐N/A
Attachment 11 – Third Party and/or Internal Security Testing Results (e.g. vulnerability assessment reports, penetration testing reports, Security Threat and Risk Assessment (STRA) documentation)	☐Yes ☐No
Attachment 12 * - Governance Structure for Data Matching (required where applicable)	☐Yes ☐N/A
Attachment 13 * – Data Matching Agreement (required where applicable)	☐Yes ☐N/A
Attachment 14 *- Data Matching PIA Addendum for Unique Collection, Use or Disclosure by a public body (required where applicable)	☐Yes ☐N/A
Attachment 15 * - Governance Structure for Common and Integrated Programs or Services (required where applicable)	☐Yes ☐N/A
Attachment 16 * - Common or Integrated Programs or Services Agreement (required where applicable)	☐Yes ☐N/A
Attachment 17 * – Common or Integrated Programs or Services PIA Addendum for Unique Collection, Use or Disclosure by a public body (required where applicable)	☐Yes ☐N/A
Attachment 18 – Algorithm Impact Assessment	☐Yes ☐No ☐N/A

PRIVACY MANAGEMENT PROGRAM

Schedule B - Information Sharing Agreement

If your initiative includes or will be part of a regular and systematic exchange of personal information with partners in or outside of the Town of Grimshaw, you may require an information sharing agreement.

Please provide information about your ISA and once complete, submit to the Privacy Officer.

Description of ISA:

Name of Town Department involved:

Any other ministries, agencies, public bodies or organizations involved:

Business Contact title and phone number for person responsible for maintaining the ISA:

ISA Start Date:

ISA End Date: