Village of Foremost

Privacy Management Program (PMP)

Version: 1.0

Approved: May 19, 2026
Next review: One year from approval

1. Purpose and Legislative Authority

This Privacy Management Program (PMP) outlines how the Village of Foremost manages and protects personal information as required under the Protection of Privacy Act (POPA) and the Access to Information Act (ATIA). It establishes the Village's privacy responsibilities, safeguards, and procedures for the proper handling of personal information.

2. Scope

This Privacy Management Program (PMP) establishes the governance structure, processes, safeguards, and responsibilities required under the Protection of Privacy Act (POPA), the Access to Information Act (ATIA), and their Regulations.

This program applies to:

- Council members
- Employees
- Contractors, service providers and volunteers
- Any individual acting on behalf of the Village

The Village applies a privacy by design approach, ensuring privacy considerations are integrated into the planning, development, and operation of all programs, services, and systems. Anyone who collects, uses, discloses, accesses, or manages personal information for Village purposes must follow this program and all related policies, procedures, and controls. Supporting guidance for staff is provided through the Village's Privacy Staff Manual, which complements this program by outlining practical procedures and expectations.

3. Definitions

The following definitions apply throughout this Privacy Management Program and its appendices. Where terms are defined in POPA, ATIA, or their Regulations, those definitions apply.

Access to Information Act (ATIA) means the provincial legislation that establishes a right of access to Records held by public bodies and sets requirements for access requests, corrections, timelines, and fees.

Administrative Safeguards means policies, procedures, and administrative measures used to protect personal information, including staff training, access controls, privacy protocols, and monitoring processes.

Automated Decision-Making System means a system that uses algorithms, artificial intelligence (AI), or automated processing to make decisions or recommendations about an individual.

Collection means the act of gathering, acquiring, or obtaining personal information by any means, as permitted under POPA.

Consent means voluntary agreement by an individual for the collection, use, or disclosure of their personal information, whether written, electronic, or oral, as recognized in the POPA Regulation.

Contractor or Service Provider means any external individual or organization that collects, uses, stores, processes, or disposes of personal information on behalf of the Village and is subject to privacy obligations under POPA and this Program.

Correction Request means a request made under POPA section 7 for correction of personal information if an individual believes the information is inaccurate, incomplete, or misleading.

Data Matching means the comparison or linking of personal information from different programs, systems, databases, or public bodies for the purpose of making decisions or verifying information, as defined under POPA.

Delegation means the written assignment of authority by the head of public body to a Privacy Officer to perform specific access or privacy duties under POPA and ATIA.

Directory of Personal Information Banks means the public-facing summary of personal information held by the Village, including the type of information, the individuals it relates to, and the purposes for which it is collected, used, and disclosed.

Disclosure means making personal information available or accessible to another individual, organization, public body, or the public, whether intentionally or unintentionally.

Employee or Staff means permanent, temporary, part-time, casual, volunteer, or contract staff working for or on behalf of the Village of Foremost.

Personal Information means recorded information about an identifiable individual, as defined under POPA and ATIA, including information that directly or indirectly identifies an individual.

Privacy Breach means an incident where personal information is accessed, used, disclosed, lost, or disposed of in an unauthorized manner.

Privacy Incident means an event involving personal information that may or may not result in unauthorized access, use, disclosure, loss, or harm. Privacy incidents include near-misses.

Privacy Impact Assessment (PIA) means a documented assessment that evaluates the privacy impacts of a program, project, system, or activity and identifies required mitigation measures, as required under POPA and ATIA.

Privacy Management Program (PMP) means the coordinated framework of policies, procedures, safeguards, training, monitoring, and governance required under POPA for managing and protecting personal information.

Privacy Officer means the CAO or an individual delegated under POPA section 55 to administer the PMP and ensure compliance with POPA and ATIA.

Protection of Privacy Act (POPA) means the provincial legislation governing the collection, use, disclosure, retention, and protection of personal information by public bodies in Alberta.

Record means information in any form, including written, digital, photographic, or audio-visual material, but not including software or mechanisms used to produce records.

Real Risk of Significant Harm means the legal threshold under POPA for determining whether notification to affected individuals and the OIPC is required following a privacy breach.

Retention Period means the defined period during which records containing personal information must be maintained before secure destruction, as set out in the Village's Records Retention and Disposal Bylaw.

Security Safeguards means administrative, physical, and technical measures used to protect personal information from unauthorized access, use, disclosure, modification, loss, or destruction.

Third-Party Data Processor means any external contractor or service provider engaged to collect, process, store, or destroy personal information on behalf of the Village.

Use means managing, applying, utilizing, or analyzing personal information within the Village for authorized purposes.

4. Governance Structure

The Village has established a privacy governance model to ensure clear accountability for compliance with POPA and ATIA. The authority for the Privacy Officer is established in the Village of Foremost Protection of Privacy and Access Governance Bylaw.

4.1 Privacy Officer

The Privacy Officer is the Head of the Public Body (CAO) or an individual designated by written delegation under section 55 of the Protection of Privacy Act. The Privacy Officer is the primary authority responsible for the Village's compliance with POPA and ATIA.

The Privacy Officer:

- Oversees and maintains the Privacy Management Program
- Manages privacy incidents and breach notifications
- Reviews and approves Privacy Impact Assessments (PIAs)
- Maintains the Directory of Personal Information Banks
- Responds to access and correction requests
- Provides privacy guidance and training
- Ensures safeguards are implemented and followed
- Liaises with the Office of the Information and Privacy Commissioner (OIPC)
- Reports to Council as required

The Privacy Officer may delegate routine administrative tasks in writing; however, overall accountability for compliance remains with the Head of the Public Body. All delegations of authority are documented in writing and align with the statutory powers and responsibilities set out under POPA and ATIA.

4.2 Council and Administration

Council supports privacy compliance by:

- Approving related bylaws and policies
- Ensuring the Privacy Officer is designated as required under POPA
- Receiving updates on privacy risks or significant incidents

Council does not participate in the day-to-day administration of access or privacy matters.

Administration supports compliance by:

- Following established privacy procedures
- Reporting privacy concerns or incidents immediately
- Cooperating with PIAs, training, and safeguard requirements

5. Directory of Personal Information Banks

The Village of Foremost maintains a Directory of Personal Information Banks in accordance with the *Protection of Privacy Act (POPA)*.

The Directory provides a public-facing summary of the personal information held by the Village, including the purposes for which it is collected, used, and disclosed.

The Directory supports compliance with POPA, ATIA, and applicable Regulations by:

- identifying the categories of personal information held by the Village;
- describing the individuals to whom the information relates;
- documenting the purposes and legal authority for collection, use, and disclosure;
- supporting transparency and accountability to the public; and
- assisting in the identification of appropriate safeguards and privacy practices.

For each Personal Information Bank, the Directory includes, at a minimum:

- the title and location of the personal information bank;
- a description of the program, service, or activity;
- the types of personal information involved;
- the categories of individuals the information relates to;
- the purpose for which the information is collected, used, and disclosed;
- the legal authority for collection;
- the general storage method or system; and
- a description of use and disclosure practices.

The Directory of Personal Information Banks is maintained by the Privacy Officer and is:

- reviewed at least annually; and
- updated when a new program, service, or activity involving personal information is introduced or significantly changed.

The Directory of Personal Information Banks is provided in Appendix B and is made available to the public in accordance with POPA.

6. Collection, Use & Disclosure Policy

The Village of Foremost collects, uses, and discloses personal information only as authorized under POPA, ATIA, and applicable Regulations.

Detailed operational procedures, templates, and forms supporting this section are documented in supporting manuals and appendices, including the Village's Privacy Staff Manual, which provides practical guidance for day-to-day staff compliance. The Village maintains an understanding of its personal information holdings through documented programs, services, and records, which support the Directory of Personal Information Banks and overall compliance with privacy legislation.

6.1 Collection

The Village collects personal information only where authorized under section 4 of POPA**.**

When personal information is collected directly from an individual, the Village provides a collection notice in accordance with POPA section 5**,** which includes:

- the purpose of the collection;
- the legal authority for the collection;
- the title and contact information for questions; and

Where applicable, whether the personal information will be used in an automated system to generate content or make decisions, recommendations, or predictions.

Approved collection notices are available in Appendix G.

6.2 Use

Personal information is used only:

- for the purpose for which it was collected;
- for a purpose that is consistent with the original purpose of collection; or
- as otherwise authorized by law.

Access to personal information is restricted to employees and service providers who require the information to perform their assigned duties.

6.3 Disclosure

The Village discloses personal information only as authorized under section 13 of the Protection of Privacy Act, including where:

- the individual has provided consent, where permitted;
- the disclosure is consistent with the original purpose of collection;
- the disclosure is authorized or required by another enactment; or
- the disclosure is made to another public body as authorized by law.

Where personal information is disclosed to service providers or third parties, appropriate contractual and safeguard requirements are applied.

6.4 Records and Administrative Documentation

Records created in the course of Village business may contain personal information.

The Village ensures that personal information contained in such records is collected, used, and disclosed only as authorized under POPA and ATIA.

Prior to public release or disclosure, records are reviewed to ensure that personal information is limited to what is necessary and authorized by law. Where required, personal information may be withheld or redacted in accordance with applicable legislation.

Original records are not altered. Any redaction or withholding is applied only to copies released or published.

6.4.1 Records Retention and Disposal

The Village of Foremost manages records in accordance with Records Retention Bylaw No. 558, as amended from time to time. All records, including records containing personal information, must be retained, stored, archived, and disposed of in accordance with the retention periods and procedures established by the bylaw.

Where personal information has been used to make a decision that directly affects an individual, the Village will retain that personal information for a minimum of one year after it is used, in accordance with applicable legislation and the Records Retention Bylaw.

Records scheduled for destruction must be destroyed securely and in accordance with the destruction and documentation requirements established by the bylaw.

6.5 Privacy Complaints

Individuals may submit privacy complaints regarding the collection, use, or disclosure of personal information.

The Privacy Officer will:

- acknowledge receipt within a reasonable time;
- review and investigate the complaint;
- document findings and corrective actions; and
- provide a written response to the complainant.

Individuals may request a review by the Office of the Information and Privacy Commissioner (OIPC) if unsatisfied with the outcome.

6.6 Data Matching & Derived Data

The Village may conduct data matching activities only where authorized under POPA.

Data matching involves linking personal information from multiple sources to create data derived from personal information. These activities are strictly controlled to protect individual privacy.

The Village ensures that:

- data matching is conducted only for authorized purposes, such as program administration, analysis, or service delivery;
- personal information used in data matching is limited to what is necessary;
- data derived from personal information is used only for the purpose for which it was created;
- data derived from personal information is not disclosed except as permitted under legislation;
- a Privacy Impact Assessment (PIA) is completed where required; and
- data derived from personal information is securely destroyed or converted to non-personal data once it is no longer required for its original purpose.

Access to data matching processes and outputs is restricted to authorized personnel.

6.7 Non-Personal Data

The Village may create and use non-personal data in accordance with the Protection of Privacy Act. Non-personal data is information that has been anonymized or modified so that it does not identify an individual. The data quality assurance process must be replicable and auditable to support transparency and compliance.

When creating non-personal data, the Village ensures that:

- the personal information used is already in its custody or control;
- appropriate methods are used to anonymize or de-identify the data;
- a data quality assurance process is applied to ensure accuracy, consistency, and reliability;
- potential risks of re-identification are assessed and mitigated; and
- documentation is maintained describing the source data, purpose, and method of anonymization.

Non-personal data may be used for purposes such as analysis, planning, and program evaluation. Non-personal data must be assigned an appropriate security classification level based on residual risk.

Where non-personal data is disclosed to a third party, the Village ensures that:

- the disclosure is authorized under legislation;
- conditions are established to protect the data, including security and confidentiality requirements;
- re-identification is prohibited; and
- the data is destroyed or returned once it is no longer required.

7. Access and Correction Requests

Individuals have the right to request access to records and to request correction of personal information in accordance with the ATIA and POPA.

7.1 Access Requests

Individuals may request access to records containing their personal information or general information by submitting a written request to the Privacy Officer.

Upon receiving a request, the Privacy Officer will:

- acknowledge receipt of the request;
- provide reasonable assistance to clarify or narrow the request, where appropriate;
- locate and review records;
- assess applicable exceptions, exclusions, or third-party information; and
- provide a written response within the timeframes prescribed by ATIA.

The Village may require proof of identity before releasing personal information and may apply extensions, fees, or other provisions as permitted under the Act and its Regulations.

Access to records is provided in the manner determined by the Village in accordance with legislative requirements.

The Access to Information Form is provided in Appendix E.

7.2 Correction Requests

The Village will respond to requests for correction of personal information in accordance with sections 7 and 8 of the Protection of Privacy Act (POPA).

- Individuals may request correction of their personal information where they believe there is an error or omission.
- Requests must relate to factual information. Opinions, including professional or evaluative opinions, will not be corrected.

Where a correction is accepted:

- the correction will be made to all relevant records; and
- the record will include an annotation indicating the date of the correction.

Where a correction is refused:

- the Village will annotate or link the personal information with the requested correction;
- the Village will notify any person or organization to whom the information was disclosed in the previous year, unless doing so is not reasonably possible or would be unduly burdensome; and
- the applicant will be notified in writing of the decision within 30 business days.

The Request for Correction of Personal Information Form is provided in Appendix F.

8. Privacy Impact Assessments (PIAs)

Privacy Impact Assessments are a key component of the Village's Privacy Management Program. A Privacy Impact Assessment (PIA) is a formal process used to identify, assess, and mitigate privacy risks associated with a new or substantially changed administrative practice, program, system, or service involving personal information.

The Village ensures that:

- PIAs align with and reference this Program;
- privacy risks identified through PIAs are addressed through policies, procedures, and safeguards; and
- PIAs support continuous improvement of privacy practices and compliance.

8.1 When a PIA is Required

A Privacy Impact Assessment is required where the Village introduces a new, or makes a substantial change to an existing, administrative practice, program, system, or service that involves the collection, use, or disclosure of personal information.

Examples of activities that may require a PIA include:

- new programs or services involving personal information;
- significant changes to existing programs or systems;
- implementation of new technologies or software;
- data matching activities;
- use of automated systems to generate decisions, recommendations, or predictions;
- sharing personal information with third parties; or
- storage or access to personal information outside of Canada.

A PIA must be submitted to the Office of the Information and Privacy Commissioner (OIPC) where required under the Protection of Privacy (Ministerial) Regulation, including where:

- personal information involved is highly sensitive;
- the project involves a significant portion of the population served;
- data matching occurs between public bodies;
- the project is part of a common or integrated program or service; or
- the project involves the use of innovative technologies, including automated systems or artificial intelligence.

Where submission is not required, the Village will still complete a PIA where prescribed and retain it for accountability purposes.

8.2 Who Completes the PIA

The Privacy Officer is responsible for:

- determining whether a Privacy Impact Assessment is required;
- coordinating the completion of PIAs;
- reviewing PIAs for completeness and compliance; and
- submitting PIAs to the OIPC where required.

Employees must notify the Privacy Officer before implementing any new or significantly changed program, system, or process involving personal information.

The Head of the Public Body, or a formally designated individual with written authority, is responsible for approving and signing Privacy Impact Assessments prior to submission to the OIPC.

8.3 PIA Process and Submission

The PIA process includes:

- describing the program, system, or activity;
- identifying the personal information involved;
- identifying legal authority for collection, use, and disclosure;
- assessing how personal information is collected, used, disclosed, stored, and retained;
- evaluating potential privacy risks; and
- identifying safeguards and mitigation measures to address those risks.

PIAs will be completed with a level of detail proportionate to the complexity, sensitivity, and risk associated with the project. Projects involving higher-risk elements, such as automated systems, data matching, or large-scale data processing, require more comprehensive analysis.

Where appropriate, the PIA process may include consultation with:

- IT or technical support providers;
- third-party vendors or service providers; and
- legal or policy advisors.

Where a project involves automated systems or artificial intelligence, the Village will assess risks related to automated decision-making, including accuracy, fairness, and oversight.

8.4 Templates and Tools

The Village will use the official Privacy Impact Assessment (PIA) Template and Completion Guide issued by the Office of the Information and Privacy Commissioner (OIPC) for all PIAs.

As of May 1, 2026, any PIA submitted to the Commissioner must be completed using the prescribed OIPC template. Submissions that do not use the required template may be deemed incomplete and will not be accepted for review.

The Village will ensure that the most current version of the template is used for each PIA.

Internal tools or checklists may be used to support completion of a PIA; however, the final PIA must be documented using the OIPC template.

8.5 Retention and Review of PIAs

Completed PIAs are maintained by the Privacy Officer in accordance with the Village's records retention requirements.

PIAs will be:

- reviewed and updated where changes to the program, system, or activity occur; and
- made available to the Office of the Information and Privacy Commissioner upon request.

9. Safeguards and Security Controls

The Village of Foremost protects personal information through administrative, physical, and technical safeguards that are reasonable and proportionate to the sensitivity and classification of the information.

Safeguards are designed to protect personal information against unauthorized access, use, disclosure, modification, loss, or destruction and are reviewed and updated as risks, technologies, and operational practices change.

9.1 Administrative Safeguards

Administrative safeguards include policies, procedures, and practices that support the secure handling of personal information, including:

- role-based access controls;
- privacy training and awareness;
- confidentiality requirements for employees, contractors, and volunteers; and
- documented processes for Privacy Impact Assessments, privacy incidents, and breach response.

9.2 Physical Safeguards

Physical safeguards are used to protect records and systems containing personal information and may include controlled access to offices and storage areas, secure storage of records, and secure disposal practices.

Physical safeguards are implemented based on the sensitivity of the information and operational requirements.

9.3 Technical Safeguards

Technical safeguards are used to protect electronic systems and records containing personal information and may include access controls, authentication measures, secure networks, monitoring, and backup and recovery processes.

Technical safeguards apply to all electronic systems, including cloud-based services used by the Village.

9.4 Information Sensitivity and Classification

The Village classifies personal information based on sensitivity to determine appropriate safeguards.

Higher-sensitivity information requires stronger safeguards and more restricted access. Classification is considered when implementing safeguards, conducting Privacy Impact Assessments, and responding to privacy incidents.

Classification	Examples	Minimum Safeguards
Low	Public contact info	Basic access controls
Medium	Utilities billing, tax accounts	Role-based access, locked storage
High	Financial info	Restricted access

Information classification is assigned at the time of collection or creation by staff, based on the sensitivity of the information. Where classification is unclear, staff must consult the Privacy Officer. Classification requirements follow POPA Regulation section 6(1)(c).

9.5 Automated Decision Making and AI

Where automated systems, including artificial intelligence, are used to assist with decisions, recommendations, or predictions involving personal information, the Village ensures that:

- the use of such systems is transparent and appropriate to the purpose;
- individuals are informed at the time of collection where their personal information will be used in an automated system, in accordance with POPA;
- human oversight is maintained over decisions that may impact individuals;
- personal information used in automated systems is accurate, relevant, and protected; and
- risks related to bias, fairness, and data quality are considered and mitigated.

9.6 Service Providers and Third Parties

Where personal information is handled by service providers or third parties on behalf of the Village, appropriate contractual and safeguard requirements are applied to ensure compliance with POPA, ATIA, and this Program.

Service providers are required to notify the Village of any privacy incident involving personal information under their control. The Village may require confirmation of compliance, conduct reviews, or request evidence of safeguards from service providers to ensure ongoing protection of personal information.

Required contract clauses are available in Appendix H.

10. Privacy Breach Management

A privacy breach occurs when personal information is accessed, used, disclosed, lost, or disposed of in a manner that is not authorized under the Protection of Privacy Act.

All suspected or confirmed privacy breaches must be reported immediately to the Privacy Officer.

10.1 What Counts as a Breach

A breach may include but is not limited to:

- unauthorized access to personal information;
- unauthorized use or disclosure;
- loss or theft of records or devices;
- misdirected correspondence; or
- improper disposal of records.

10.2 Breach Response Steps

Upon becoming aware of a privacy breach, the Privacy Officer will:

- contain the breach and limit further unauthorized access or disclosure;
- investigate the circumstances of the breach;
- identify the personal information involved;
- assess the risk of harm to affected individuals;
- document findings and corrective actions; and
- implement measures to prevent similar incidents from occurring.

10.3 Notification Requirements (POPA)

Notification content will comply with the Protection of Privacy (Ministerial) Regulation and will include required details such as the nature of the breach, dates, types of personal information involved, mitigation steps taken, contact information, and an individual's right to request a review by the Commissioner.

Notification to affected individuals and the OIPC is required when the breach creates a Real Risk of Significant Harm, which may include:

- identity theft;
- financial loss;
- discrimination or harm to reputation; or
- loss of employment or opportunities.

Notification to affected individuals, the Office of the Information and Privacy Commissioner (OIPC), and the Minister responsible for the Protection of Privacy Act will occur without unreasonable delay where a Real Risk of Significant Harm has been identified.

10.4 Staff Responsibilities

All staff, Council members, contractors, and volunteers must:

- report suspected or confirmed breaches immediately;
- preserve all relevant records and information;
- follow instructions from the Privacy Officer; and
- complete additional training if required.

10.5 Documentation

The Privacy Officer maintains records of:

- reported privacy breaches and incidents;
- risk assessments and notification decisions;
- corrective actions taken; and
- measures implemented to prevent recurrence.

Lessons learned from privacy breaches are used to improve safeguards, training, and procedures.

10.6 Privacy Incidents vs Privacy Breaches

Not all privacy incidents result in a confirmed privacy breach.

All reported privacy incidents are assessed by the Privacy Officer to determine whether unauthorized access, use, disclosure, loss, or harm has occurred.

Where an incident is determined to meet the definition of a privacy breach, the Village will follow the formal breach response and notification requirements outlined in this Program.

11. Training & Awareness

The Village of Foremost provides privacy training to ensure that individuals who handle personal information understand their obligations under POPA, ATIA, and this Privacy Management Program.

11.1 Training Requirements

Privacy training is mandatory for:

- all new employees as part of onboarding;
- Council members;
- temporary, seasonal, and volunteer staff who handle personal information; and
- contractors or service providers, where appropriate.

Training includes:

- privacy obligations under applicable legislation;
- identification and protection of personal information;
- secure handling and safeguarding practices;
- reporting privacy incidents and breaches; and
- collection notice and consent requirements, where applicable.

The Village's Privacy Staff Manual is used as a core training and reference tool to support staff in applying privacy requirements in their daily work. Privacy training is mandatory upon onboarding and refreshed at least annually.

11.2 Refresher Training

Individuals who handle personal information must complete refresher privacy training at intervals determined by the Village, and at least once every year, or sooner where:

- legislative or policy changes occur;
- new systems or technologies are introduced; or
- privacy incidents indicate a need for additional training.

11.3 Training Records

The Privacy Officer maintains records of privacy training, including:

- training content;
- dates of completion; and
- acknowledgements by participants.

Training records are maintained to demonstrate compliance and support audits or reviews.

11.4 Ongoing Awareness

The Privacy Officer promotes ongoing privacy awareness through guidance, reminders, and updates when new programs, systems, or privacy risks are identified.

12. Monitoring and Review

The Village of Foremost monitors its privacy practices to ensure ongoing compliance with POPA, ATIA, and this Privacy Management Program.

12.1 Monitoring Responsibilities

The Privacy Officer is responsible for monitoring the Village's privacy practices, including:

- reviewing how personal information is handled across programs and services;
- ensuring safeguards are implemented and followed;
- maintaining privacy-related documentation; and
- identifying emerging privacy risks.

12.2 Annual Review

This Privacy Management Program is reviewed at least once per year and may be reviewed sooner where:

- legislative or regulatory changes occur;
- new systems, technologies, or programs are introduced; or
- privacy incidents or risk assessments indicate a need for updates.

Supporting procedures, templates, and appendices may be updated administratively by the Privacy Officer to reflect operational or legislative changes.

12.3 Continuous Improvement

The Village applies lessons learned from privacy incidents, audits, and reviews to improve safeguards, training, and privacy practices on an ongoing basis. The Privacy Officer may update procedures, forms, or appendices at any time to:

- strengthen safeguards
- address risks
- reflect operational changes
- incorporate best practices

Substantive changes to the Privacy Management Program framework may be brought forward to Council for approval, where required.

13. Public Disclosure and Contact

In accordance with section 25(3) of the Protection of Privacy Act, the Village of Foremost will make this Privacy Management Program available to the public:

- on the Village website; and/or
- upon request, within 30 business days.

When providing the Privacy Management Program, the Village may withhold technical, security-related, or other sensitive information where disclosure could reasonably be expected to compromise the security of personal information or systems.

Where applicable, staff manuals, guidelines, or reference materials used in decision-making processes may be made available to the public in accordance with the Access to Information Act, subject to any required severing of protected information.

Public inquiries regarding this Privacy Management Program or privacy practices should be directed to:

Privacy Officer
Village of Foremost
Email: office@foremostvillage.ca
Phone: 403-867-3733

Appendices

The following documents form part of the Privacy Management Program and may be updated by the Privacy Officer without amending the Program.

Appendix A	Delegation of Authority
Appendix B	Directory of Personal Information Banks
Appendix C	Privacy Impact Assessment (PIA)
Appendix D	Privacy Breach Report Form
Appendix E	Access to Information Form
Appendix F	Request for Correction of Personal Information Form
Appendix G	Collection Notice Library
Appendix H	Third-Party Privacy Contract Clauses

VILLAGE OF FOREMOST

Box 159
Foremost, Alberta
T0K 0X0
e-mail: vlg4most@telusplanet.net
Telephone (403)867-3733 ***Fax (403)867-2031***

December 1, 2025

Kassidy Millington
Box 53
Foremost, Alberta
T0K 0X0

Re: Delegation of Authority – Appointment as Privacy Officer under POPA

Dear Kassidy,

Pursuant to Section 55 of the Protection of Privacy Act (POPA) and Section 6(1)(a) of the Protection of Privacy (Ministerial) Regulation, I, Marilynn Hirsche, CAO and Head of the Public Body for the Village of Foremost, hereby delegate to you the authority and responsibilities of the Privacy Officer for the Village of Foremost.

This delegation authorizes you to act as Privacy Officer, for all duties and functions required under POPA, the Access to Information Act (ATIA), and all associated Regulations. As Privacy Officer, you are authorized to:

1. Administer and oversee the Village's Privacy Management Program (PMP), including all associated policies, procedures, inventories, training, and documentation.
2. Coordinate, review, and approve Privacy Impact Assessments (PIAs) as required under POPA/ATIA.
3. Respond to all privacy-related inquiries, including those from members of the public, staff, Council, contractors, and the Office of the Information and Privacy Commissioner (OIPC).
4. Manage privacy breaches, including intake, investigation, containment, mitigation, documentation, reporting, and notification to affected individuals and/or the OIPC in accordance with POPA.
5. Coordinate access and correction requests related to personal information holdings.
6. Maintain and oversee the Personal Information Inventory, privacy documentation, records retention alignment, and compliance tracking.
7. Develop, deliver, and document staff privacy training and awareness activities.
8. Recommend policy updates and improvements to the CAO and Council as required.
9. Carry out all additional responsibilities assigned under POPA, ATIA, and Regulations, as amended from time to time.

Yours truly,

Marilynn Hirsche
CAO

Directory of Personal Information Banks

Appendix B – Privacy Management Program

The Village of Foremost maintains the following Directory of Personal Information Banks in accordance with the *Protection of Privacy Act (POPA)*. This directory provides a high-level summary of personal information held by the Village and the purposes for which it is collected, used, and disclosed.

1. Utility Billing Records

Description: Records related to utility accounts and billing
Individuals: Utility customers (residents/property owners)
Personal Information: Name, address, account number, billing history, payment info
Purpose: Billing, account management, collections
Authority: Municipal Government Act
Storage: Excel, financial system, paper files
Use/Disclosure: Internal; may be disclosed for collections or legal enforcement

2. Property Tax Records

Description: Property ownership and taxation records
Individuals: Property owners
Personal Information: Name, address, roll number, tax amounts, payment history
Purpose: Tax administration and collection
Authority: Municipal Government Act
Storage: Tax system, Excel, paper files
Use/Disclosure: Internal; may be shared for enforcement or audit

3. Accounts Receivable (AR)

Description: Non-utility receivables and invoicing
Individuals: Residents, businesses, organizations
Personal Information: Name, contact info, account details, balances
Purpose: Billing and payment tracking
Authority: Municipal Government Act
Storage: Accounting system, Excel
Use/Disclosure: Internal; collections/legal if required

4. Payroll & Employee Records

Description: Employment and payroll information
Individuals: Employees
Personal Information: Name, SIN, banking info, pay records, benefits
Purpose: Payroll, HR administration
Authority: Employment Standards Code, Income Tax Act
Storage: Payroll system, secure files
Use/Disclosure: Internal; required disclosures to CRA, benefits providers

5. Accounts Payable (AP)

Description: Vendor and payment records
Individuals: Vendors (if sole proprietors**)**
Personal Information: Name, address, banking/payment info
Purpose: Payment processing
Authority: Municipal Government Act
Storage: Accounting system
Use/Disclosure: Internal; financial audit

6. Cemetery Records

Description: Burial and plot ownership records
Individuals: Deceased individuals and purchasers
Personal Information: Names, plot location, purchase info
Purpose: Cemetery management
Authority: Cemeteries Act and Municipal Government Act
Storage: Paper records, Excel, maps
Use/Disclosure: Public inquiries (limited), internal

7. Bylaw Enforcement Records

Description: Complaints and enforcement actions
Individuals: Residents, complainants, subjects of complaints
Personal Information: Name, address, complaint details
Purpose: Enforcement of municipal bylaws
Authority: Municipal Government Act
Storage: Files, email, reports
Use/Disclosure: Internal; may be disclosed for legal proceedings

8. Council & Governance Records

Description: Council meeting materials and correspondence
Individuals: Council members, residents
Personal Information: Names, contact info, correspondence content
Purpose: Governance and decision-making
Authority: Municipal Government Act
Storage: Agendas, minutes, digital files
Use/Disclosure: Public records (with redactions where required)

9. Recreation / Facility Bookings

Description: Program registrations and bookings
Individuals: Residents, participants
Personal Information: Name, contact info, booking details
Purpose: Program delivery and scheduling
Authority: Municipal Government Act
Storage: Forms, spreadsheets
Use/Disclosure: Internal

10. General Inquiries & Correspondence

Description: Emails, calls, and public inquiries
Individuals: Members of the public
Personal Information: Name, contact info, message content
Purpose: Responding to inquiries
Authority: Municipal Government Act
Storage: Email systems
Use/Disclosure: Internal

Privacy Breach Report Form

Report Details	
Date of Report:	Reported By:
Department:	Role:
Incident Details	
Date Incident Occurred:	
Location of Incident:	
Individuals Involved:	
Description of Incident:	
How was this Incident Discovered?	
Personal Information Involved	
Type (e.g., name, address, accounts):	
Approx. Number of Affected Individuals:	
Sensitivity Level:	○ LOW ○ MEDIUM ○ HIGH
Cause of Breach	
Cause (check one)	○ Accidental Disclosure ○ Unauthorized Access ○ Loss / Theft ○ Unknown
Internal or External:	Was Malicious Intent Suspected? ○ Yes ○ No
Containment Measures	
Actions Taken to Contain and Mitigate the Incident:	

Risk Assessment			
Potential Risk of Harm:			
Likelihood of Harm:	○ LOW	○ MEDIUM	○ HIGH
Other Risk Considerations:			

Notifications	
Affected Individuals Notified? ○ Yes ○ No	Method: ○ In Person ○ Phone Call ○ Email
If No, Why?	
OIPC Notification Required? ○ Yes ○ No	Date OIPC Notified:

Prevention / Follow-Up		
Actions Taken to Prevent Reoccurrence:		
Policy/Procedure Changes Required?	○ Yes ○ No	○ TBD
Additional Staff Training Required? ○ Yes ○ No	Date Scheduled:	

Additional Notes

FOR OFFICE USE ONLY	
Privacy Officer Signature:	Date:
Notes:	

ACCESS TO INFORMATION ACT (ATIA)
ACCESS TO INFORMATION REQUEST

The personal information collected on this form is collected under the authority of the Access to Information Act (ATIA) and section 4 of the Protection of Privacy Act (POPA), and will be used for the purpose of responding to your access to information request. If you have any questions about the collection or use of this information, please contact the Privacy Officer at office@foremostvillage.ca or 403-867-3733.

SECTION 1: APPLICANT INFORMATION	
First Name:	Last Name:
Company or Organization (if applicable):	
Mailing Address:	
Phone Number:	Email:

SECTION 2: REQUEST DETAILS	
1. What kind of information do you want to access?	
○ General Information (An initial fee of $25 is required)	○ Your own Personal Information (no fee required)
2. How do you want to receive the information?	○ By Email ○ By Mail ○ Examine the records
3. What records do you want to access? Please give as much detail as possible.	
4. If inquiring about a specific property, what is the address?	
5. What is the time period of the records? Please give specific dates.	

SECTION 3: STATEMENT OF APPLICANT

By submitting this request form, I confirm that:

1. I am the above-named Applicant.
2. The information provided on this application is true, complete and correct.

_____ Signature

_____ Date

Please submit your completed request form to the Village of Foremost Privacy Officer

Email: office@foremostvillage.ca

Mail: PO Box 159, Foremost AB T0K 0X0

In Person: 301 Main Street, Foremost AB T0K 0X0

FOR OFFICE USE ONLY	
Date Received:	Received By:
Request Number:	Initial Fee: ○ N/A ○ $25 Receipt No: _____

Access to Information Form Instructions

You can access many public body records without making a request under the Access to Information Act. To determine whether you need to make a request under the Act or if you need help completing the form, contact the Privacy Coordinator.

How to make a request
To obtain access to a record, a request must:
- be in writing;
- be submitted to the public body the applicant believes has custody or control of the record;
- provide enough detail to enable the public body to locate and identify the record within a reasonable time with reasonable effort; and
- be accompanied by a fee where a fee is required under this Act.

The Village of Foremost should respond to the request within 30 business days from receiving the request, unless the time to respond to a request has been extended for additional reasonable purposes.

Applicant Information
In this part of the form enter:
- your full name;
- the name of the company or organization you are representing, if applicable;
- your complete mailing address and contact information so that the Privacy Officer can contact you about the request;
- an e-mail address, if any, where correspondence may be sent.

Request Information

1. Type of request
Check Personal Information or General Information
A request for general information is information other than your own personal information. For example, information about a third-party.
- There is an initial fee of $25.00;
- Additional fees may apply for more complex requests;
- The records are provided when the fee is paid in full.

A request for personal information is recorded information about an identifiable individual. A request for personal information can only be made for your own personal information or for personal information of an individual you are entitled to represent.
- There is no initial fee for accessing your own personal information.

2. Do you want to receive a copy of the record or examine the record?
Check the appropriate box indicating whether you want to receive a copy of the record or examine the record.

3. What records do you want to access?
- Be as specific as possible in describing records.
- If you need more space, continue your description on a separate sheet of paper and attach it to this request form.

If requesting your own personal information, give:
- Your full name;
- Any other names that you have previously used.

If requesting another person's information, give:
- The person's full name;
- any other names that person may have used on the records;
- proof that you have the authority to act for that person (e.g. power of attorney).

4. What is the time period of the records?
Enter the specific dates or date ranges of the records you want to access (e.g. if you want records for the period of January 1, 2025 to August 31, 2025, etc.)

Your signature Sign and date the form.

Where to send your request
Send your completed form, and initial fee if applicable, to the Privacy Officer.

ACCESS TO INFORMATION ACT (ATIA)
CORRECTION OF PERSONAL INFORMATION REQUEST

The personal information collected on this form is collected under the authority of section 4 of the Protection of Privacy Act (POPA) and will be used for the purpose of responding to your request for correction of personal information. If you have any questions about the collection or use of this information, please contact the Privacy Officer at office@foremostvillage.ca or 403-867-3733.

SECTION 1: APPLICANT INFORMATION	
First Name:	Last Name:
Company or Organization (if applicable):	
Mailing Address:	
Phone Number:	Email:

SECTION 2: REQUEST DETAILS

1. **Whose information do you want to correct?**

   ○ Your own Personal Information

   ○ Another person's information (attach proof of legal authority)

2. **What personal information needs to be corrected?** Please give as much detail as possible. Be sure to give the complete name that is in the records if it is different from the name given above.

3. **What correction do you wish to make and why?** Please attach any supporting documents.

SECTION 3: STATEMENT OF APPLICANT

By submitting this request form, I confirm that:

1. I am the above-named Applicant.
2. The information provided on this application is true, complete and correct.

_____ Signature

_____ Date

Please submit your completed request form to the Village of Foremost Privacy Officer

Email: office@foremostvillage.ca

Mail: PO Box 159, Foremost AB T0K 0X0

In Person: 301 Main Street, Foremost AB T0K 0X0

The Village will respond to your request within 30 business days as required under the Protection of Privacy Act (POPA).

FOR OFFICE USE ONLY	
Date Received:	Received By:
Request Number:	

The Village of Foremost is required under the *Protection of Privacy Act (POPA)* and the *Access to Information Act (ATIA)* to provide notice when collecting personal information. This appendix provides approved collection notice wording for use on Village forms.

G.1 Standard Collection Notice (General Use)

This notice is used on all Village forms (paper or electronic) where personal information is collected, unless a program-specific notice below is required.

"The personal information collected on this form is collected under the authority of section 4 of the Protection of Privacy Act (POPA) and will be used for the purpose of ***[state purpose]****. It may be disclosed to* ***[state recipients, if any]*** *as required to administer this program or activity. If you have any questions about the collection or use of this information, please contact the Privacy Officer at office@foremostvillage.ca or 403-867-3733."*

G.2 Example Collection Notices (Program-Specific)

The following program-specific notices may be used in place of the standard notice where appropriate.

Program/Activity	Purpose of Collection	Disclosures (if applicable)	Approved Collection Notice
Utility Billing	Administer utility services, billing, payments, and account records	Auditors; contracted billing service providers	*"The personal information collected for utility billing is collected under section 4 of the Protection of Privacy Act (POPA). It is used to administer utility services, issue invoices, process payments, and maintain account records. Information may be disclosed to the Village's auditors or contracted service providers for billing administration. For questions, contact the Privacy Officer at office@foremostvillage.ca or 403-867-3733."*
Property Taxes / Assessment Roll	Levy property taxes and maintain assessment records	Alberta Land Titles; assessor; authorized tax agents	*"The personal information collected for property taxation and assessment is collected under the Municipal Government Act and section 4 of the Protection of Privacy Act (POPA). It is used to levy taxes, maintain assessment records, and communicate with property owners. Some information may be disclosed to Alberta Land Titles, the Village assessor, or authorized tax agents as required by law. Questions may be directed to the Privacy Officer at office@foremostvillage.ca or 403-867-3733."*
Employment Applications	Assess suitability for employment	Hiring personnel	*"Personal information collected through this employment application is collected under section 4 of the Protection of Privacy Act (POPA) and will be used to assess your suitability for employment with the Village of Foremost. It may be disclosed to individuals involved in the hiring process. Successful applicants will have this*

			information transferred to their personnel file. For questions, contact the Privacy Officer at office@foremostvillage.ca or 403-867-3733."
Recreation / Campground Bookings	Manage reservations and registrations	None	*"The personal information collected for recreation or campground bookings is collected under section 4 of the Protection of Privacy Act (POPA). It is used to manage reservations, issue confirmations, and contact registrants as required. For questions about this collection, contact the Privacy Officer at office@foremostvillage.ca or 403-867-3733."*
Bylaw Enforcement / Complaints	Investigate and enforce bylaws	Law enforcement; regulatory authorities	*"The personal information collected for bylaw enforcement is collected under the Municipal Government Act, relevant Village bylaws, and section 4 of the Protection of Privacy Act (POPA). It will be used to investigate and resolve bylaw matters and may be disclosed to law enforcement or other authorities where necessary to enforce legislation. For questions, contact the Privacy Officer at office@foremostvillage.ca or 403-867-3733."*
Website Submissions (Contact Forms, Requests, Online Inquiries)	Respond to inquiries	None	*"The personal information collected through this online form is collected under section 4 of the Protection of Privacy Act (POPA). It will be used to respond to your inquiry and administer Village programs or services. For questions regarding the collection or use of this information, contact the Privacy Officer at office@foremostvillage.ca or 403-867-3733."*

Third-Party Privacy Contract Clause

Appendix H – Privacy Management Program

The following clauses must be included in all contracts, service agreements, procurement documents, and vendor arrangements where a third party may have access to personal information on behalf of the Village of Foremost.

These clauses ensure compliance with the Protection of Privacy Act (POPA), the Access to Information Act (ATIA), and the Village's Privacy Management Program (PMP).

The Privacy Coordinator may update these clauses as required without amending the PMP.

H.1 Required Contract Clauses

1. Compliance with Legislation

The Contractor agrees to comply with the Protection of Privacy Act (POPA), the Access to Information Act (ATIA), and all applicable privacy, security, and information management requirements established by the Village of Foremost.

2. Use of Personal Information

The Contractor shall collect, use, and access personal information **only as necessary** to perform the services described in this Agreement and for no other purpose.

3. Disclosure Restrictions

The Contractor shall not disclose any personal information to any third party unless:
(a) expressly authorized in writing by the Village; or
(b) required by law.

4. Safeguards

The Contractor shall protect personal information through reasonable administrative, physical, and technical safeguards appropriate to the sensitivity of the information. Safeguards must prevent unauthorized access, use, disclosure, alteration, or destruction.

5. Storage and Access

Personal information must be stored securely and accessed only by individuals who require access to perform the contracted services.
The Contractor must notify the Village before storing personal information outside Alberta or Canada.

6. Breach Reporting

The Contractor must immediately notify the Village of any suspected or confirmed privacy breach, security incident, or unauthorized access to, use of, or disclosure of personal information.
Notification must occur **within 24 hours** of discovery.

7. Cooperation with Investigations

The Contractor shall fully cooperate with the Village in:

- breach investigations
- reporting obligations
- audits
- inquiries from the Office of the Information and Privacy Commissioner (OIPC)

8. Subcontracting

The Contractor shall not subcontract services involving personal information without the prior written approval of the Village.

All approved subcontractors must abide by the same privacy obligations.

9. Retention and Disposal

Upon completion of the contract, termination, or upon request by the Village:

(a) personal information must be returned to the Village; or

(b) securely destroyed in a manner approved by the Village.

The Contractor must provide written confirmation of destruction if requested.

10. Right of Audit

The Village reserves the right to audit the Contractor's privacy and security practices related to this Agreement to confirm compliance.

11. Confidentiality

The Contractor agrees to keep all personal information confidential and shall ensure that all employees, agents, and subcontractors are bound by equivalent confidentiality obligations.

12. Notification of Changes

The Contractor must notify the Village of any change in ownership, security practices, or system changes that may affect personal information protection.

13. Indemnification

The Contractor shall indemnify and hold harmless the Village of Foremost from any damages, losses, penalties, or liabilities resulting from the Contractor's failure to comply with these privacy requirements.

H.2 Guidance for Staff (Internal Use)

Village administration should insert these clauses into:

- service provider agreements
- recreation management software contracts
- IT system contracts
- cloud service agreements
- consultants with access to personal information
- any outsourcing arrangement (billing, communications, website hosting)

When unsure, staff must consult the Privacy Officer.