Procedure Title: **Privacy Management Program**
Policy: **1200-09**
Adopted: **June 16, 2026**
Resolution No.: **2026.06.16/09**
Amended:

POLICY STATEMENT

The Village of Mannville is committed to protecting the Personal Information of its residents, ratepayers, and employees. The Village will ensure that privacy protection is core consideration in the design, implementation and evolution of all Village programs and services.

The collection, use, and disclosure of Personal Information may only be undertaken within the parameters of the *Protection of Privacy Act* (POPA) and the *Access to Information Act* (ATIA). The Village will ensure that appropriate measures are in place to govern the collection, use and disclosure of Personal Information by establishing a Privacy Management Program.

1.0 REASON FOR POLICY

1.1 To ensure compliance with POPA, Section 25 which requires that each public body establish and maintain a Privacy Management Program.
1.2 To promote accountability by establishing clear roles, responsibilities, and process for managing privacy risks.
1.3 To foster trust by demonstrating a commitment to privacy.
1.4 To specify safeguards to protect Personal Information, data derived from personal and non-personal information.
1.5 To enable risk management tools to identify, assess, and mitigate privacy risks proactively.

2.0 RELATED INFORMATION

2.1 *Access to Information Act* (ATIA), SA 2024, c. A-1.4
2.2 *Access to Information Regulation*, Alta Reg 133/2025
2.3 *Protection of Privacy Act* (POPA), SA 2024, c. P-28.5
2.4 *Protection of Privacy (Ministerial Regulation*, Alta Reg 143/2025
2.5 *Protection of Privacy Regulation*, Alta Reg 132/2025
2.6 Government of Alberta Data and *Information Security Classification Guideline,* 2021

3.0 DEFINITIONS

3.1 **ATIA** means the Access to Information Act (ATIA), SA 2024, c. A-1.4

3.2 **Commissioner** means the Information and Privacy Commissioner.

3.3 **Council** means the governing body for the Village of Mannville comprised of 5 individual Councillors whom have been elected to office for a four-year term.

3.4 **Employee** means a person who works for the Village of Mannville. This includes Village staff, and anyone working for the Village as an appointee, volunteer, student, service provider, contractor, or agent.

3.5 **Non-Personal Data** means data, including data derived from Personal Information, which has been generated, modified, or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the regulations.

3.6 **Personal Information** means recorded information about an identifiable individual, including:

3.6.1 the individual's name, home or business address, home or business telephone number, home or business email address, or other contact information, except where the individual has provided the information on behalf of the individual's employer or principal in the individual's capacity as an employee or agent;

3.6.2 the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;

3.6.3 the individual's age, gender identity, sex, sexual orientation, marital status or family status;

3.6.4 an identifying number, symbol or other particular assigned to the individual;

3.6.5 he individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;

3.6.6 information about the individual's health and health care history, including information about the individual's physical or mental health;

3.6.7 information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;

3.6.8 anyone else's opinions about the individual; and

3.6.9 the individual's personal views or opinions, except if they are about someone else.

3.7 **PIA** means a Privacy Impact Assessment as described in Section 8.0 of this Policy, and mandated under POPA Section 26.

3.8 **PIB** means the Village of Mannville Personal Information Bank as described in Section 9.0 of this Policy and mandated under POPA Section 57.

3.9 **PMP** means the Village of Mannville Privacy Management Program.

3.10 **POPA** means the Protection of Privacy Act (POPA), SA 2024, c. P-28.5.

3.11 **Privacy Breach** means an incident involving the loss of unauthorized access to or unauthorized disclosure of Personal Information in the custody or under the control of the Village where a reasonable person would consider that there exists a real risk of significant harm (RROSH) to an individual as a result of the loss, unauthorized access or unauthorized disclosure. This includes all Personal Information as defined under POPA Section 1{q) and Section 1{e).

3.12 **Privacy Officer** means the CAO or their designate to oversee the Village of Mannville's Privacy Management Program.

4.0 RESPONSIBILITIES

4.1 Village Council to:

- 4.1.1 Approve by resolution this policy and any amendments.
- 4.1.2 Consider the allocation of resources for successful implementation of this policy in the annual budget process.

4.2 Chief Administrative Officer (CAO) to:

- 4.2.1 Implement this policy and approve procedures.
- 4.2.2 Ensure policy and procedure reviews occur and verify the implementation of policies and procedures.
- 4.2.3 Designate a Privacy Officer for the Village.

4.3 Director/Manager of the Department to:

- 4.3.1 Ensure implementation of this policy and procedure.
- 4.3.2 Ensure that this policy and procedure is reviewed every three years.
- 4.3.3 Make recommendations to the Chief Administrative Officer of necessary policy or procedure amendments.
- 4.3.4 Understand, and adhere to this policy and procedure.
- 4.3.5 Ensure employees are aware of this policy and procedure.

4.4 Privacy Officer

4.4.1 Develop, implement and maintain a Privacy Management Program (PMP) for the Village of Mannville.

4.4.2 Ensure all tasks and responsibilities set out in the PMP are incorporated in the organizational structure.

4.4.3 Report to the CAO on compliance with POPA and any privacy risks and mitigation strategies.

4.5 All Employees to:

4.5.1 Understand and adhere to this policy and procedure.

5.0 PRIVACY OFFICER

5.1 The contact information for the designated Privacy Officer will be made available on the Village website.

6.0 ACCESS TO INFORMATION

6.1 In accordance with Part 1, Division 1 of ATIA, applicants may access records in the Village's custody or control, including an individual's own Personal Information, subject only to the limitations defined within ATIA.

6.1.1 Access to information requests must be submitted to the Privacy Officer in writing and accompanied by the prescribed fee.

6.2 In processing all requests for information, the Village will:

6.2.1 Exercise a duty to assist by responding to applicants openly, accurately, and completely, making every reasonable effort to facilitate the location and retrieval of records;

6.2.2 Respond to the applicant within 30-business days. The Village may utilize extensions under Section 16 of ATIA, only when qualitatively or quantitatively necessary; and

6.2.3 Collect fees only as permitted by ATIA and regulations.

6.3 The Privacy Officer, or their delegate, retains the authority to:

6.3.1 Request clarification to enable a record search;

6.3.2 Transfer requests to more appropriate public bodies; or

6.3.3 Disregard requests in accordance with Section 9 of ATIA.

7.0 COLLECTION, USE, AND DISCLOSURE

7.1 Personal Information may only be collected, used, or disclosed for the purposes for which it was collected.

7.2 The Village must provide notice to the individual at the time of collection that includes:

- 7.2.1 The purpose for which the information is collected;
- 7.2.2 The specific legal authority for the collection;
- 7.2.3 The email address, telephone number, or other contact information for the Privacy Officer; and
- 7.2.4 The Village's intention, if any, at the time to input the information into an automated system to generate content or make decisions, recommendations, or predictions.

7.3 If the Village plans to use or disclose Personal Information in any way that was not indicated in the collection notice, the individual must provide consent. Acceptable consent must be submitted by the individual:

- 7.3.1 in writing if it is signed by the individual who is giving the consent; or
- 7.3.2 electronically through the Village of Mannville website.

7.4 Any individual may withdraw their consent at any time by providing written notice.

8.0 PRIVACY IMPACT ASSESSMENTS

8.1 A Privacy Impact Assessment (PIA) must be completed for any new, or a substantial change to an existing, administrative practice, program, project or service that will involve the collection, use or disclosure of Personal Information if:

- 8.1.1 A loss, unauthorized access, or disclosure of the information could cause real risk of significant harm (RROSH); or
- 8.1.2 The PIA is mandated to be completed and submitted to the Commissioner.

8.2 The Director, Manager, or Supervisor is responsible for identifying each practice, program, project or service that may require a PIA. The Privacy Officer will provide support to all employees who must complete a PIA.

- 8.2.1 A Director, Manager or Supervisor may request that a third-party service provider complete a PIA as part of the procurement process.

8.3 A PIA must include:

8.3.1 A summary of the purpose of the collection, use, or disclosure of Personal Information;

8.3.2 The types of Personal Information that will be collected, used or disclosed and the security arrangements in place to protect the Personal Information;

8.3.3 The legal authority for the collection, use or disclosure of the Personal Information;

8.3.4 Any privacy risks and mitigation strategies respecting the Personal Information;

8.3.5 Any administrative, physical or technical safeguards in place to protect the Personal Information, including how the Personal Information will be securely transmitted, matched or linked by the Village, if applicable;

8.3.6 Any accuracy, correction and retention procedures that will be implemented to ensure the Personal Information is accurate and complete; and

8.3.7 A clear structure outlining the responsibilities and accountability of each public body if two or more public bodies are engaging in a common or integrated program/service or if the Village is collecting Personal Information from another public body for the purpose of data matching.

8.4 If the Village has already completed a PIA for an existing practice, program, project, or service, it can amend that PIA instead of creating a new one, if the updated version still meets the requirements identified in POPA and regulations.

8.5 If two or more public bodies are working together on a shared program, service, or data-matching project, they may prepare one joint PIA. Each public body must also complete an addendum to cover any unique ways it collects, uses, or discloses Personal Information.

8.6 A PIA must be submitted to the Commissioner if one or more of the following apply to the practice program, project, or service:

8.6.1 It will handle highly sensitive Personal Information;

8.6.2 It will use Personal Information from a large portion of the Village residents;

8.6.3 It involves data matching with another public body.

8.6.4 It is part of a shared or integrated program or service.

8.6.5 It uses new or innovative technology.

8.6.6 The Commissioner specifically asks for the PIA.

9.0 PERSONAL INFORMATION BANK

9.1 The Privacy Officer will establish and maintain an inventory of Personal Information collected by the Village that includes:

- 9.1.1 The program, system, or activity used to collect Personal Information;
- 9.1.2 The department within the organization responsible for collecting and maintaining the Personal Information;
- 9.1.3 The purpose for which the Personal Information is collected, including any legislative authority to collect Personal Information;
- 9.1.4 A list of the specific Personal Information that is collected;
- 9.1.5 The method in which the Personal Information is collected;
- 9.1.6 Confirmation that the collection notice is up to date and included on the collection method;
- 9.1.7 Identification of all departments/employee positions with access to the Personal Information;
- 9.1.8 Identification of where records are stored and their retention schedule; and
- 9.1.9 Any and all safeguards in place to protect Personal Information.

9.2 All Personal Information identified within the Personal Information Bank will be assigned a security classification level as outlined in Section 16.0 of this Policy.

9.3 A directory of the PIB will be made available to the public in accordance with POPA Section 57.

10.0 REQUEST FOR CORRECTION OF PERSONAL INFORMATION

10.1 Any individual who believes there is an error or omission in their individual Personal Information may submit a request for correction to the Village.

- 10.1.1 Requests for correction applies only to factual information, not opinions of the individual.
- 10.1.2 The individual must provide proof in support of the request that is of the same nature and at least the same quality as the Personal Information required when the original collection took place.

10.2 The respective Village department will review the request for correction to determine is the Personal Information is correctable.

10.2.1 If the Personal Information can be corrected, the Village will make the correction.

10.2.2 If the Personal Information cannot be corrected, the Village will annotate or link the record with the individual's request for correction.

10.3 When a correction, annotation, or link is made, the Village will notify any other public body or third party who received the information within the past one (1) year.

10.3.1 The Village does not need to notify other public bodies or third parties if:

i. The correction, annotation, or link is not material; and

ii. The individual who requested the correction is advised and agrees in writing that notification is not necessary.

10.3.2 If another public body is notified, they must also make the correction, annotation, or link in their records.

10.4 Within thirty (30) business days, the Village will notify the individual in writing whether:

10.4.1 The correction was made; or

10.4.2 An annotation, or link was made instead.

11.0 RESPONDING TO PRIVACY INCIDENTS

11.1 All Privacy Breaches must be reported, tracked, assessed, responded to, and reviewed in accordance with the Village of Mannville Privacy Breach Procedure.

11.2 The Privacy Officer will assess each Privacy Breach to determine the real risk of significant harm (RROSH) to an individual as a result of the Privacy Breach.

11.3 If a Privacy Breach meets the threshold for RROSH, the Privacy Officer will, without unreasonable delay, notify:

11.3.1 The individual to whom there exists a real risk of significant harm;

11.3.2 The Commissioner; and

11.3.3 The Minister, in accordance with POPA Section 10(2).

12.0 RESPONDING TO PRIVACY COMPLAINTS

12.1 An individual has the right to submit a complaint to the Commissioner if the individual believes their Personal Information has been collected, used or disclosed improperly.

12.2 Before an individual (the complainant) can submit a request for review to the Commissioner, the complainant must submit the complaint to the Village.

12.3 If the Village decides to respond to the complaint, the Village must respond within thirty (30) days after the complaint was received.

12.4 After the thirty (30) day response period, the complainant can submit the complaint in writing to the Commissioner:

12.4.1 Within sixty (60) days of the Village's response; or

12.4.2 If the Village did not respond, sixty (60) days from the end of the thirty (30) day response period.

13.0 CREATION, USE, AND DISCLOSURE OF NON-PERSONAL DATA

13.1 The Village can only create non-personal data from Personal Information or data derived from Personal Information if it is already in the Village's custody or control.

13.2 The Village may create, use, and disclose non-personal data for the purposes of:

13.2.1 Statistical reporting;

13.2.2 Operational data;

13.2.3 Financial and budget data;

13.2.4 Geographic or environmental data;

13.2.5 Program evaluation data; or

13.2.6 Any other authorized purpose identified in POPA Section 21(1).

13.3 Any creation, use or disclosure of Non-Personal Data must be done in accordance with the Village's Non-Personal Data Procedure.

13.4 A record of each assessment where Non-Personal Data has been created, used, or disclosed must be retained by the Privacy Officer.

14.0 ARTIFICIAL INTELLIGENCE (AI)

14.1 The Village of Mannville permits the use of Al tools, including Large Language Models (LLMs), as a productivity and research aid to support administrative tasks.

14.2 Employees using third-party Al tools are prohibited from inputting, uploading, or disclosing any of the following:

- 14.2.1 Personal Information;
- 14.2.2 Confidential or privileged information;
- 14.2.3 Non-public organizational information;
- 14.2.4 Information related to identifiable individuals, including residents, employees, contractors, elected officials or service providers; and
- 14.2.5 Information subject to legal, contractual, or security restrictions.

14.3 Employees are fully responsible for reviewing the entire contents of any information derived from Al tools for completion, accuracy, and biases.

15.0 AUTOMATED SYSTEM USE OF PERSONAL INFORMATION

15.1 The Village may use automated systems, including information systems, software applications, and artificial intelligence-enabled tools, to support service delivery, administrative functions, analysis, and decision-making.

15.2 Personal Information may only be used in automated systems if:

- 15.2.1 The use is authorized under ATIA and POPA.
- 15.2.2 The use is necessary for an operating program or activity; and
- 15.2.3 The use is consistent with the purpose for which the Personal Information was originally collected.

15.3 Where Personal Information is used in automated systems to make or support decisions, recommendations, or predictions that may have an impact on individuals, the Village must:

- 15.3.1 ensure that the use of such systems is documented and approved by the CAO;
- 15.3.2 ensure that human oversight will be maintained to review outputs and decisions; and
- 15.3.3 provide individuals with information about the use of the automated systems involving their Personal Information.

15.4 Prior to implementing or significantly modifying an automated system that uses Personal Information, a Privacy Impact Assessment will be completed in accordance the Section 6.0 of this Policy.

16.0 SECURITY CLASSIFICATION SYSTEM

16.1 All documents and records containing Personal Information, data derived from Personal Information and Non-Personal Data must be assigned a security classification level.

16.1.1 The Village of Mannville will utilize the Government of Alberta Data and Information Security Classification Guideline in determining the necessary security classification levels.

16.2 Unless otherwise determined, all documents and records will automatically be assigned the highest security classification level.

16.3 Security Classification Levels:

Level	Description
PUBLIC	Applies to data and information that, if compromised, will not result in injury to individuals, governments, or to private sector institutions.
PROTECTED A	Applies to data and information that, if compromised, could cause injury to an individual, organization, or government.
PROTECTED B	Applies to data and information that, if compromised, could cause serious injury to an individual, organization, or government.
PROTECTED C	Applies to data and information that, if compromised, could cause extremely grave injury to an individual, organization, or government.

16.4 It is the responsibility of each employee to understand that as data or information moves through the information management lifecycle, or as the context in which it exists changes, the applied security classification level may need to be re-assessed.

16.4.1 If the security classification of Personal Information, data derived from Personal Information and Non-Personal Data has been re-assessed, the employee must notify the Privacy Officer so the Personal Information Bank may be updated.

17.0 SAFEGUARDS

17.1 Village employees must ensure that any collection, use, or disclosure of Personal Information is supported by appropriate safeguards.

17.1.1 Safeguards may be administrative, technical, or physical, and will be selected based on the sensitivity of the Personal Information and the level of risk. Examples of safeguards are provided in Appendix A.

18.0 PRIVACY MANAGEMENT PROGRAM TRAINING

18.1 Mandatory training will be provided to all employees by the Privacy Officer or their delegate to ensure that all employees:

18.1.1 Understand their role and responsibilities as employees of a public body;
18.1.2 Can identify Personal Information and confidential organizational information;
18.1.3 Understand the rules related to the collection, use, disclosure, retention, and safeguarding of Personal Information;
18.1.4 Recognize privacy risks and potential Privacy Breaches; and
18.1.5 Know how and when to seek guidance from the Privacy Officer.

18.2 All current employees must complete Privacy Management Program training within ninety (90) days of approval of this policy.

18.3 All new employees must complete Privacy Management Program training within the first thirty (30) days of their employment.

18.4 Refresher training will be conducted for each department every two (2) years or when legislation or policy changes.

18.4.1 Managers may request additional training as needed.
18.4.2 The Privacy Officer may assign additional training as needed.

18.5 Training completion will be documented and tracked by the Privacy Officer or their delegate.

19.0 THIRD-PARTY SERVICE PROVIDERS

19.1 Third-party service providers and contractors are considered Employees. As such, third-party service providers and contractors must abide by the requirements of this policy.

19.2 If a third-party service provider or contractor has access to Personal Information within the custody or control of the Village of Mannville, they must provide, in writing, confirmation of the following considerations:
- 19.2.1 Control and accountability measures;
- 19.2.2 Legal authorities for collection, use, or disclosure;
- 19.2.3 Requests for access or correction;
- 19.2.4 Use of Artificial Intelligence (Al) or automated systems;
- 19.2.5 Safeguards and retention;
- 19.2.6 Complaints handling; and
- 19.2.7 Termination of contract.

19.3 All considerations identified in Section 19.2 of this policy must be captured in the contract agreement.

20.0 TRANSITION

20.1 Any reference to the Freedom of Information and Protection of Privacy Act (FOIP Act) in existing policies, procedures, forms, or other organizational documents shall be deemed to be a reference to the Access to Information Act (ATIA), SA 2024, c A-1.4 and the Protection of Privacy Act (POPA), SA 2024, c P-28.5, as applicable. All such documents will be reviewed and amended to reflect the correct legislative titles as soon as practicable.

21.0 REVIEW

21.1 This Policy and corresponding Procedures must be reviewed at least every three (3) years to ensure alignment with best practices and legislative requirements, or sooner if required due to legislative changes.

22.0 APPENDIX

22.1 Appendix A: Personal Information Protection Safeguards

22.2 1200-09-01: Privacy Breach Procedure

23.0 END OF POLICY

Procedure Title: **Privacy Management Program**
Policy: **1200-09**
Adopted: **June 16, 2026**
Resolution No.: **2026.06.16/09**
Amended:

APPENDIX 'A' PERSONAL INFORMATION PROTECTION SAFEGUARDS

This list provides examples of Personal Information protection safeguards that may be considered when collecting, using, or disclosing Personal Information. It is not an exhaustive list. Employees should consult with their manager and the Privacy Officer when considering the collection, use, or disclosure of Personal Information to ensure that appropriate risks and safeguards are identified and addressed.

Physical Safeguards	Administrative Safeguards	Technical Safeguards
• Restricted access to offices, records rooms, and server locations • Locked filing cabinets and secure storage for paper records • Key card, fob, or controlled key access to facilities • Clean desk and secure document disposal practices (e.g., shredding) • Secure off-site storage for records • Visitor sign-in and escort requirements	• Privacy policies, procedures, and guidelines • Role-based access authorization and approval processes • Privacy and security training for employees and contractors • Confidentiality agreements and code of conduct requirements • Records retention and secure destruction schedules • Incident response and breach management procedures • Privacy Impact Assessments for new or significantly changed programs • Contractor and service provider privacy and security requirements	• User authentication (e.g., passwords, multi-factor authentication) • Role-based system access controls • Encryption of Personal Information at rest and in transit • System logging, monitoring, and audit trails • Firewalls, intrusion detection, and malware protection • Secure system configuration and patch management • Automatic session timeouts and device locking • Secure backup and recovery systems