



Department: Administration

Policy No: 20

Policy Title: Privacy Management Policy (PMP)

Resolution No: 120/26

Date: May 20, 2026

Review Date: 2028

Village of Alix Privacy Management Policy (PMP)

Purpose statement:

The purpose of the PMP is to:

- Ensure compliance with the requirements, principles and intent of the *Protection of Privacy Act (PoPA)* to foster public trust and confidence.
- Ensure the privacy and protection of personal information by establishing the roles, responsibilities, principles and practices on how it is collected, retained, accessed, used, disclosed and disposed.
- Define roles and responsibilities of municipal employees, elected officials, contractors, consultants, and volunteers related to the management of personal information.

Scope:

This policy applies to Village of Alix (Village) employees, elected officials, contractors, consultants, volunteers, public boards and agencies and to all personnel who have access to personal information that is in the custody or control of the Village. This policy does not apply to employees' personal information.

Policy:

1. Collection of personal information

The Village shall only collect personal information that is required to provide its programs and services. Wherever possible, such information will be collected directly from the individual about whom it pertains. The amount and the type of information collected will be limited to that which is needed to fulfil the identified purpose(s).

Prior to the collection of personal information, the Village must obtain consent from affected individuals for particular uses and disclosures of personal information prior to the collection of the information unless legislation permits otherwise. Where possible, consent will be expressed (rather than implied) and in writing.

Whenever the Village collects personal information, a notice of collection shall be provided with, or in advance of collection and obtain explicit consent from the affected individual, unless the legislation permits otherwise.

The notice of collection must include the following information:

- 1.1 The legal authority that permits the collection of the personal information;
- 1.2 The purposes for which the personal information is being collected, used, retained and disclosed; and
- 1.3 The name, title and direct contact information for an individual who can answer questions about the specific collection, use, protection and disposal of personal information.

Wherever practical, notices of collection are provided in written format. Verbal notices of collection can be used for service interactions where written notices are impractical, such as telephone interactions. Implied consent may be obtained under some circumstances (e.g., a notice is posted in a publicly available space to inform individuals that their image may be captured where photography or videography is taking place, and they elect to enter the space).

2. Use and disclosure of personal information

The Village will ensure that personal information is used only for the purpose for which it was collected, for a consistent purpose, when the individual to whom the personal information relates consents to another purpose, or in accordance with PoPA. The Village will take reasonable steps to ensure the accuracy of personal information in its records.

Personal information will only be disclosed in accordance with legislative requirements outlined in PoPA and Village procedures. Where disclosure is not clearly authorized under the legislation, the Village will obtain the express consent of the affected individual prior to doing so. Whenever personal information will be shared with third parties, the Village will ensure that an agreement with provisions to protect personal information in accordance with this policy, related internal procedures, and PoPA are in place prior to any information being shared.

3. Protection of personal information

Personal information must be secured from the point of collection to the point of destruction. The Village will make reasonable effort to protect personal information from loss, theft, unauthorized access, use, disclosure, modification or destruction through appropriate administrative, technical, and physical security measures and safeguards. Access to personal information within the Village will be restricted to those staff members who need the information to carry out their duties. The Village will ensure that third party service providers adhere to this policy and include the requirement for similar level of protection in the contractual agreements. The Village's additional methods of protection include:

- 3.1 Staff training on privacy and the protection of personal information;
- 3.2 Granting access to information on a need-to-know basis;
- 3.3 Technical measures such as passwords, audit trails and firewalls;
- 3.4 Physical measures such as secured vaults and restricted access to stored information.

4. Access to and correction to personal information

Individuals have a right to access their own personal information within a record that is in the custody or control of the Village, subject to legislated exemptions and exceptions outlined in PoPA. Village staff must verify the identity of persons requesting access to their own personal information before granting access.

Village staff will accept and process a request for correction to an individual's personal information where the individual demonstrates there are inaccuracies or incomplete information and is able to provide proof.

5. Public record redaction of personal information

5.1 Individuals may request additional redaction of their personal information from public facing documents before or after publication by submitting a written request. Requests must:

- a. Clearly identify the information to be redacted (e.g., provide a website link, meeting date, or screenshot).
- b. Provide a rationale outlining the reason for the request for redaction.

5.2 The Village will review requests on a case-by-case basis, considering:

- a. The presence or absence of a statutory requirement for disclosure.
- b. Any evidence that the individual has taken prior steps to limit public access to their information.
- c. The balance between public transparency and personal privacy protection.
- d. The availability of alternative solutions to mitigate harm.

5.3 The Village will not redact personal information required by provincial statutes unless there is a compelling, legally justified reason.

5.4 In cases where individuals provide detailed and compelling justification of safety risks (e.g., documented harassment, court orders, law enforcement concerns), the Village will prioritize removing or redacting requested personal information.

5.5 Decisions to redact personal information from public facing documents will be reviewed and approved or denied by the CAO or their designate.

5.6 If the Village grants a redaction request and amends its content, it will not take further action to remove the information from other sources (e.g., third-party websites, search engine caches). Individuals must pursue such actions independently.

5.7 To maintain compliance with legislation, unredacted records may still be available for in-person viewing upon request.

6. Retention and destruction of personal information

The Village will only retain personal information for as long as necessary to fulfil the stated purpose as identified at the time of collection and PoPa in order to provide an individual with a reasonable opportunity to access their personal information.

Personal information will be disposed of in accordance with the Village's Record Retention Policy, authorized destruction procedures and in a secure manner that prevents loss, misuse, theft, or unauthorized access given its format.

7. Privacy breach and complaints

The Village takes privacy breaches seriously and investigates each suspected or actual breach. Staff members must immediately report all suspected or known privacy breaches or complaints to their supervisor and the Office of the Information and Privacy Commissioner (OIPC) upon discovery.

The Access to Information Coordinator shall conduct breach management activities as described in the Privacy Incident Response Procedure, attached as Schedule “A”, to determine the nature and scope of the breach.

8. Definitions:

For the purpose of this Policy, unless otherwise stated, the following definitions apply:

“disclosure” means the release of personal and confidential information by any method (i.e. sharing information by any means such as verbally, sending an email, posting online) to any person.

“disposition” means the action taken with regards to personal and confidential information including destruction, transfer to another entity, or permanent preservation.

“Protection of Privacy Act SA 2024, c P-28.5” or “PoPA” means provincial legislation as amended and includes any regulations passed under it, governing the collection, use and disclosure of information by certain institutions in Alberta including municipalities.

“personal information” means personal information as defined under the Protection of Privacy Act SA 2024, c P-28.5 as amended.

“business information” means information associated with an individual in a professional, business, or official capacity that is not personal information. Examples include name, position, title, business telephone number, and business email of an individual.

“privacy” means a set of interests and rights that an individual has regarding their ability to control the collection, use, disclosure and disposal retention of their own personal information that is in the custody or under the control of the Village. Privacy is not an absolute right in all situations. Personal information may be collected, used, disclosed or retained without the consent of individuals where specific legislation permits.

“privacy breach” means when personal information is collected, retained, used, disclosed or disposed in ways that are not in accordance with the provisions of PoPA and/or municipal policies.

“record” means a record as defined in the Access to Information Act, as amended.

“use” means the purpose(s) for which the information was obtained or compiled.

9. Responsibilities

The Village is responsible for the personal information that we collect, retain, use, disclose, and destroy. The Village will continue to develop policies and practices to ensure that personal information is handled in strict accordance with legislation.

10. All employees and volunteers:

10.1 Maintain the protection of personal information they collect, retain, use, disclose and dispose of for Village business in all work environments and locations where Village business is conducted;

10.2 Where work duties include access to personal information, take privacy awareness and training to understand their responsibility to protect privacy in executing their operational duties;

10.3 Understand and adhere to their access and privacy responsibilities as noted in this procedure and other Village policies and procedures;

10.4 Report any actual or suspected privacy breach arising from unauthorized, inadvertent collection use, or disclosure of personal information to the Access to Information Coordinator.

11. Managers and supervisors:

Along with the responsibilities noted above:

11.1 Be accountable for ensuring personal information is collected, used, disclosed and disposed in accordance with legislation and associated regulations, standards and other Village policies, and for compliance with this policy;

11.2 Implement this policy and communicate requirements to employees under their direction;

11.3 Respond to requests for records from the Access to Information Coordinator in relation to access to personal information requests;

11.4 Ensure proper notice is given and/or the required level of consent is obtained prior to the collection or use of all personal information;

11.5 Restrict access to personal information to those individuals who require access to personal information in order to perform their duties and where access is necessary for the administration of their business;

11.6 Require vendors and contractors to comply with this policy and that privacy rules and concerns are referenced in all procurement documents where personal information will be processed;

11.7 Require that employees, vendors and contractors maintain a level of privacy awareness appropriate with their responsibilities;

11.8 Inform employees of the legal and administrative consequences of any inappropriate or unauthorized access to, or collection, use, disclosure, or disposition of, personal information related to a particular program, service or activity;

11.9 Ensure privacy impact assessments are conducted prior to implementation of any new technology, system, program or service involving the collection, use, disclosure or disposition of personal information.

11.10 Report any actual or suspected privacy breach arising from unauthorized, inadvertent collection use, or disclosure of personal information to the Office of the Information and Privacy Commissioner.

12. The Access to Information Coordinator, will:

12.1 Act as the Head under PoPA and as provided for through Council delegation;

12.2 Be accountable for overseeing the administration of PoPA and for decisions made under the above legislation;

12.3 Ensure oversight of and compliance with this policy;

12.4 Develop and implement policies, programs and services to ensure awareness of access to information processes and protection of personal information as necessary;

12.5 Investigate and respond to complaints regarding the misuse of personal information or reports of privacy breaches following the Privacy Incident Response Procedure;

12.6 Provide recommendations and sign-off on any privacy impact assessments prior to the implementation of a new application, system, program or service involving the collection or use of personal information or personal health information;

12.7 Ensure that legislative updates are incorporated into the Village's collection, use and disclosure processes;

12.8 Be responsible for the receipt, coordination, response and sign off for all formal information requests received pursuant to PoPA in collaboration with all departments; and

12.9 Assist the public with requests for access to information as required.

_____ (Mayor)

_____ (CAO)

_____ (Date)

Schedule “A”

Privacy Incident Response Procedure

Designed to effectively manage and respond to privacy-related incidents, ensure compliance and minimize risks.

Overview of the Procedure:

1. **Preparation and Planning:** Education on compliance requirements and training staff to recognize and report privacy incidents promptly.
2. **Incident Detection and Reporting:** Staff should be trained to identify potential privacy incidents and report them immediately. This includes unauthorized access to personally identifiable information or cybersecurity breaches.
3. **Incident Assessment:** Once an incident is reported, the Access to Information Coordinator assesses the situation to determine the severity and potential impact of the incident. This includes gathering relevant information and identifying affected data.
4. **Containment:** Implement measures to contain the incident and prevent further unauthorized access or data loss. This may involve isolating affected systems or disabling compromised accounts.
5. **Eradication:** Identify the root cause of the incident and eliminate it. This may involve removing malware, closing vulnerabilities, or addressing procedural weaknesses that led to the incident.
6. **Recovery:** Restore affected systems and data to normal operations. This includes ensuring that all systems are secure before bringing them back online.
7. **Notification:** Depending on the nature of the incident and applicable laws, notify affected individuals, regulatory bodies, and other stakeholders as required. This is crucial for compliance and maintaining trust.
8. **Documentation:** Maintain detailed records of the incident, response actions taken, and communications. This documentation is essential for compliance and for reviewing the incident later.

9. **Post-Incident Review:** Conduct a thorough review of the incident to identify lessons learned and areas for improvement. This should involve all relevant stakeholders and lead to updates in policies and procedures as necessary.
10. **Continuous Improvement:** Use insights gained from the incident and the review process to enhance the incident response plan and overall privacy practices within the organization.
11. **Compliance Monitoring:** Regularly review and update the incident response procedure to ensure compliance with evolving laws and regulations related to privacy and data protection.

By following this structured approach, the Village of Alix aims to effectively manage privacy incidents, minimize risks, and ensure compliance with legislation while protecting sensitive information and fostering trust with stakeholders.