Procedure Title: **Privacy Breach Procedure**
Policy: **1200-09-01**
Adopted: **June 16, 2026**
Resolution No.: **2026.06.16/10**
Amended:

PROCEDURE STATEMENT:

The Protection of Privacy Act (POPA) establishes requirements for the protection of personal information, data derived from personal information and non-personal data against such risks as unauthorized access, collection, use, disclosure, or destruction. Privacy Breaches may occur when information is not adequately protected.

This Procedure outlines the necessary steps when responding to a Privacy Breach.

1.0 RELATED INFORMATION

1.1 1200-09 Privacy Management Program Policy
1.2 *Protection of Privacy Act* (POPA), SA 2024, c. P-28.5
1.3 *Protection of Privacy (Ministerial) Regulation*, Alta Reg 143/2025

2.0 CONTAINMENT

2.1 As soon as a Privacy Breach is identified, the employee must immediately notify their supervisor/manager and take necessary steps to contain and document the Privacy Breach. Refer Appendix A for examples of common privacy incidents and potential containment actions.

2.2 Contact the Village's Information Technology (IT) Helpdesk or specific system support team immediately if the Privacy Breach involves an IT system/device/application that is suspected to be or has been compromised.

3.0 INITIAL REPORTING

3.1 Report the Privacy Breach to the Village's Privacy Officer by providing the following details:
- 3.1.1 Date and time the Privacy Breach occurred and/or was discovered;
- 3.1.2 Description of the Privacy Breach;
  - i. Describe the personal information involved in the Privacy Breach
  - ii. Describe how the Privacy Breach occurred
  - iii. Describe what containment actions have occurred to date.

3.2 The Privacy Officer, in consultation with the CAO, will determine if a Privacy Breach should be reported to the Village's legal representation.

3.3 If the Privacy Breach involves suspected theft or criminal activity, the Privacy Officer will contact the appropriate police agency.

4.0 INVESTIGATION AND EVALUATION OF RISK

4.1 The Privacy Officer will gather all relevant information to determine the nature and extent of the Privacy Breach.

4.2 The Privacy Officer will evaluate whether the incident meets the threshold for real risk of significant harm (RROSH) and prepare an analysis of the harm assessment.

4.2.1 In assessing the threshold for RROSH, the Privacy Officer will refer the Protection of Privacy (Ministerial) Regulation Section 4(1) and Section 4(2).

4.3 All records related to a Privacy Breach report, investigation, and evaluation will be retained by the Privacy Officer to evaluate potential trends and determine areas of improvement.

5.0 NOTIFICATION

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

5.1.1 The individual to whom there exists a real risk of significant harm;
5.1.2 The Information and Privacy Commissioner; and
5.1.3 The Minister of Technology and Innovation.

5.2 A notice to the individual to whom there exists a real risk of significant harm must be in writing and must include:

5.2.1 The name of the public body giving the notice;
5.2.2 A description of the Privacy Breach;
5.2.3 The date on which the Privacy Breach occurred;
5.2.4 The date on which the Privacy Breach was discovered;
5.2.5 A description of the personal information involved in the Privacy Breach;
5.2.6 A description of the steps taken to mitigate further risk of harm;
5.2.7 Contact information for the Privacy Officer;
5.2.8 Notice of the individual's right to request a review by the Commissioner under POPA Section 37; and
5.2.9 Other information the public body considers relevant.

5.3 A notice to the Information and Privacy Commissioner must be in writing and must include:

5.3.1 The name of the public body giving the notice;
5.3.2 A description of the Privacy Breach;
5.3.3 The date on which the Privacy Breach occurred and when it ended, or was thought to have ended;
5.3.4 The date on which the Privacy Breach was discovered;
5.3.5 The manner in which the Privacy Breach was discovered, and if applicable, the physical location of the loss or unauthorized access or disclosure;
5.3.6 A description of the personal information involved in the Privacy Breach;
5.3.7 The estimated number of individuals affected by the Privacy Breach;
5.3.8 A description of the steps taken to mitigate further risk of harm;
5.3.9 A description of the measures taken to prevent subsequent similar Privacy Breaches;
5.3.10 An example of the notice provided under Section 5.2 of this Procedure;
5.3.11 Contact information for the Privacy Officer; and
5.3.12 Other information the public body considers relevant.

5.4 A notice to the Minister must be in writing and must include:

5.4.1 The name of the public body giving the notice;
5.4.2 A description of the Privacy Breach;
5.4.3 The date on which the Privacy Breach occurred and when it ended, or was thought to have ended;
5.4.4 The date on which the Privacy Breach was discovered;
5.4.5 A description of the personal information involved in the Privacy Breach;
5.4.6 The estimated number of individuals affected by the Privacy Breach; and
5.4.7 Other information the public body considers relevant.

5.5 If the Privacy Breach does not meet the threshold for RROSH, the Privacy Officer is not obligated to provide notification.

5.6 The CAO will notify Village Council when a Privacy Breach occurs.

6.0 ADDITIONAL MEASURES

6.1 Depending on the circumstances of the Privacy Breach, the Privacy Officer may recommend additional mitigation measures.

6.2 All mitigation measure recommendations with financial implications must be approved by the CAO.

7.0 PREVENTION

7.1 The Privacy Officer will provide the CAO with recommendations on next steps, including, but not limited to, notification, additional mitigation measures, and preventative measures to prevent reoccurrence of future incidents.

7.2 Preventative measures may include, but are not limited to:

- 7.2.1 Updating policies and procedures;
- 7.2.2 Improving physical or digital security safeguards; or
- 7.2.3 Providing additional training to employees on privacy practices.

8.0 APPENDIX

8.1 Appendix A: Examples of Common Privacy Incidents and Potential Containment Actions

9.0 END OF POLICY

Procedure Title: Privacy Breach Procedure
Policy: 1200-09-01
Adopted: June 16, 2026
Resolution No.: 2026.06.16/10
Amended:

Appendix A: Examples of Common Privacy Incidents and Potential Containment Actions

Potential Privacy Breach	Potential Containment Actions
Misdirected email to wrong client/public body employee or other unintended recipient	• Request an email recall through your email system, if function is available. • Where a group email includes an untended recipient remove unintended recipient, resend email requesting staff to delete and not respond to the original email. • Contact unintended recipient, advising information was sent in error and request them to double delete the email from both their inbox and deleted box. Confirm information was not read and no copies were made.
Documents are mailed or sent to the wrong individual	• Contact unintended recipient and request the records be returned or destroyed.
Public body employee uploads documents for one client into another client's file	• Restrict access or delete the information from the uploaded information. • Review to ensure correct personal information is placed on the right file. • Contact the unintended recipient and request them to delete it on their side (if possible). • Confirm no copies of the information were made or retained.
A public body employee's work laptop and/or cellphone is stolen	• Contact appropriate team (for example cybersecurity, information technology, etc.) to request devices be remotely wiped and request them to confirm if any attempts at log-in were received after last known employee's use. • Contact law enforcement to report theft.
A public body employee accessed third party personal information (such as family members, friends, neighbors etc.) on a public body's database or file system	• Restrict access to the files. • Restrict access for the public body employee to any information.
Potential inadvertent destruction of personal information records	• Confirm and investigate missing records. • Determine if the missing records were inadvertently destroyed.