VILLAGE OF BARONS

Reference: Council Meeting	**Adopted By:** Resolution	**Number:** 088
Prepared By: Jen Durell	**Date:** June 3, 2026	**Supersedes:**

POLICY

Title: Protection of Privacy

The Purpose of This Policy is to:

a. Set out the roles, responsibilities, and general principles that The Village of Barons ("TheVillage") must follow to ensure compliance with the *Access to Information Act* (*"ATIA"*), SA 2024, Chapter A-1.4, the *Protection of Privacy Act* (*"POPA"*), SA 2024, Chapter P-28.5, and the *Protection of Privacy (Ministerial) Regulation* ("*Ministerial Regulation*"), AR 143/2025;

b. Foster public trust and confidence in The Village through openness and transparency regarding the collection and management of personal information, data derived from personal information and non-personal data;

c. Ensure The Village takes reasonable security safeguard measures to protect and manage personal information, data derived from personal information, and non-personal data in its custody or under its control against such risks of unauthorized access, collection, use, disclosure, or destruction;

d. Ensure The Village is accountable for making reasonable efforts to provide access to personal information, data derived from personal information, non-personal data and records;

e. Communicate expectations for employee conduct as one of The Village's Code of Conduct policies; and

f. Set out a Privacy Incident Response Protocol.

APPLICABILITY

This Policy applies to:

a. All employees; and

b. All records containing personal information or through which individuals can reasonably be identifiable through the mosaic effect, data derived from personal information and non-personal data, regardless of format or location, that are in the custody or under the control of The Village.

This Administration Policy does not apply to:

a. Elected officials;

POLICY STATEMENT

Personal Information

Collection of Personal Information and Notice

a. The Village only collects personal information as authorized by law, for the purposes of law enforcement or as is necessary for The Village's operating programs or activities.

b. Personal information is collected directly from the individual the information is about, subject to exceptions under *POPA*.

c. When information is collected directly from an individual, notice is given to inform them of the purpose of the collection, the legal authority for the collection, and the contact information of an individual who can answer questions about the collection, subject to exceptions under POPA.

d. When information is collected directly from an individual, notice is given, at the time of collection, of The Village's intention, if any, at that time to input the information into an automated system to generate content or make decisions, recommendations or predictions.

e. The Village is committed to providing a website that respects our visitors' privacy. Collection and management of personal information through the website is based on the legal authority and purpose expressed in the notice in accordance with *POPA*, and the Privacy Policy of the website.

Use and Disclosure of Personal Information

a. The Village may only use personal information to the extent permitted under *POPA*, or other applicable legislation.

b. The Village may only disclose personal information as permitted under *ATIA* and *POPA*, or other applicable legislation.

Sale of Personal Information

a. The selling of personal information in any circumstance or for any purpose, including for marketing or advertising purposes is prohibited.

Accuracy and Correction of Personal Information

a. The Village will make reasonable efforts to ensure that personal information used to make a decision directly affecting an individual is complete and accurate.

b. Individuals shall have the right of access to records in the custody or under the control of The Village containing their personal information.

c. Individuals may request a correction to their personal information if they believe there is an error or omission. A correction request will be handled in accordance with the Correction of Personal Information Standard.

Retention and Disposition of Personal Information

a. Where The Village uses an individual's personal information to make a decision that directly affects the individual, The Village will retain the personal information for at least one year after using it.

b. The Village will retain and dispose of records containing personal information in accordance with The Village's *Retention and Disposition Bylaw* and *Corporate Records Management Administration Policy*.

Data Matching and Data Derived from Personal Information

Collection or Creation of Data Derived from Personal Information

a. The Village may carry out data matching to create data derived from personal information only for research and analysis or planning, administering, delivering, managing, monitoring or evaluating a program or service, or as otherwise permitted under applicable law.

b. When carrying out data matching to create data derived from personal information, The Village will only collect personal information from another public body or use personal information in its custody or under its control.

Use and Disclosure of Data Derived from Personal Information

a. Data derived from personal information may only be used for the purpose for which it was created and as long as is reasonably necessary to enable The Village to carry out that purpose.

b. The Village will not disclose data derived from personal information, except to another public body from which personal information was collected for the purpose of carrying out data matching to create data derived from personal information and if that public body requires the data for the purpose for which it was created.

Retention and Disposition of Data Derived from Personal Information

a. As soon as reasonably possible, The Village will destroy data derived from personal information or transform it into non-personal information after The Village has finished using it for the purpose for which it was created.

Non-Personal Data

Creation of Non-Personal Data

a. The Village may create non-personal data only for research and analysis or planning, administering, delivering, managing, monitoring or evaluating a program or service, or as otherwise permitted under applicable law.

b. When creating non-personal data, obligations respecting the use of generally accepted best practices, quality assurance, and maintaining a creation record will be managed with the Privacy Officer.

c. To create non-personal data, The Village will only use personal information or data derived from personal information already in The Village's custody or control.

Use and Disclosure of Non-Personal Data

a. The Village may use non-personal personal data it has created for any purpose.

b. The Village may disclose non-personal data to another public body for any purpose.

c. The Village may disclose non-personal data to a person other than a public body only for the purpose of research and analysis, or planning, administering, delivering, managing, monitoring, or evaluating a program or service.

d. Any disclosure of non-personal data to a person other than a public body must be done in association with the Privacy Officer and only after the person has signed an agreement complying with the approved conditions.

e. The Village is not restricted from disclosing reports, summaries or other publications containing non-personal data that is in aggregate or statistical form.

Protection of Personal Information, Data Derived from Personal Information and Non-Personal Data

a. The Village is committed to meeting its legal obligations to have reasonable security arrangements against such risks including unauthorized access, collection, use, disclosure, or destruction of personal information, data derived from personal information, and non-personal data.

b. The Village protects personal information, data derived from personal information and non-personal data by implementing physical, technological, and/or administrative safeguards appropriate to the sensitivity of the information.

c. When an applicant makes an access to information request for their personal information, The Village will require them to provide acceptable proof to verify the applicant's identity, to show that they are the individual whose personal information is being requested.

d. All contracts entered into by The Village that may involve the collection, use, or disclosure of personal information in the performance of the contract, will include a requirement for reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

Artificial Intelligence and Automated Systems

The Village will only use personal information in artificial intelligence systems or automated systems in accordance with *POPA*.

Privacy Management Program

Privacy Management Program ("PMP")

a. The Village will establish and implement a PMP consisting of documented policies and procedures that promote The Village's compliance with its duties under *POPA*.

b. The Village shall make the PMP publicly accessible.

c. The PMP shall be reviewed, assessed and updated from time to time, but no less than every two years.

Privacy Compliance and Risk Assessment

Privacy Compliance and Risk Assessment Engagement

a. The Village will participate in Privacy Compliance and Risk Assessment engagement when a new, or a substantial change to an existing, administrative practice, program, project or service involves the collection, use or disclosure of personal information.

b. Should The Village practice, program, project or service meet *POPA* and *Ministerial Regulation* requirements for the preparation of a privacy impact assessment ("PIA") it shall provide a level of detail commensurate with the complexity of the practice, program, project or service.

c. A PIA must be submitted to the Office of the Information and Privacy Commissioner ("OIPC") if one or more factors apply, as prescribed in *POPA* and the *Ministerial Regulation*.

Privacy Incidents

Privacy Incident Response

a. The Village will investigate all privacy-related incidents and may respond to any privacy-related complaint.

b. An investigation is triggered by the submission of a *Privacy Incident Report Form*, through the direction of the OIPC, or the Privacy Officer.

c. Investigation activities may include reviewing and assessing information provided, conducting interviews and gathering evidence to document the events related to a privacy incident.

d. The Village's "Privacy Incident Response Protocol" (Appendix 1) describes the roles and responsibilities for managing privacy incidents.

ROLES AND RESPONSIBILITIES

Employees are responsible for:

a. Participating in mandatory privacy awareness training to understand appropriate collection, use, protection, management, disclosure, correction, and disposition of personal information, data derived from personal information and non-personal data;

b. Only collecting, using, and disclosing personal information as authorized by *POPA*, or other applicable legislation;

c. Implementing reasonable safeguards to protect personal information, data derived from personal information and non-personal data;

d. Participating in privacy compliance and risk assessment engagement to help identify and address potential privacy risks with respect to a 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;

e. Ensuring that the Privacy Officer is engaged in any projects involving data matching or non-personal data;

f. Responding to access to information requests in a timely manner by searching for, documenting, and producing all responsive records;

g. Reporting any privacy incidents to the Privacy Officer, and limiting the scope and impact of any privacy incident when possible;

h. Reviewing privacy recommendations and implementing the recommended privacy risk mitigation strategies where possible; and

i. Making factual corrections to personal information without a formal request under *POPA,* if this is practical and expedites public business, when directly requested by the individual whom the personal information relates to in accordance with the Correction of Personal Information Standard.

Access and Privacy Program Administrators ("APPA"s) and Alternates are responsible for:

a. Attending APPA specific training, and in consultation with the Privacy Officer, providing corresponding advice and guidance to their business unit regarding compliance with *ATIA and POPA*;

b. Seeking guidance from the Privacy Officer regarding new or complex situations involving personal information, data derived from personal information and non-personal data;

c. Ensuring that information that can be routinely disclosed is identified;

d. Participating in the Privacy Compliance and Risk Assessment engagement and facilitating the completion and maintenance of business unit inventory of privacy engagement outcomes;

e. Being the first point of contact with the Privacy Officer for any projects involving data matching or non-personal data; and

f. Conducting regular reviews to ensure compliance with *the Protection of Privacy Administration Policy*, including reporting noncompliance concerns to their director or Privacy Officer when issues arise.

Head of the Local Public Body ("the Head") is responsible for:

a. Protecting personal information by ensuring reasonable security arrangements are made against such risks as unauthorized access, collection, use, disclosure or destruction of personal information, data derived from personal information, and non-personal data as set out in *POPA;*

b. Maintaining an up-to-date delegation instrument for the Head's delegated powers and duties.

Privacy Officer is responsible for:

a. Developing and implementing policies, guidelines, and procedures to manage The Village's compliance with *POPA*;

b. Assisting with establishing and endorsing standards and procedures to ensure compliance with the privacy protection measures in *POPA* regarding the collection, use, disclosure, accuracy, retention, and safeguards of personal information, data derived from personal information, and non-personal data;

c. Ensuring the Village has policies and procedures for proactive monitoring of information systems that hold personal information, data derived from personal information, or non-personal data;

d. Policies related to the use of personal information in artificial intelligence systems, the creation of data derived from personal information and the creation of non-personal data, if The Village is using personal information in artificial intelligence systems, the creation of non-personal data or data matching activities;

e. Communicating with the OIPC, including coordinating any negotiations, mediations, inquiries, and investigations on behalf of The Village;

f. Leading the Village's training on *POPA*, policies, procedures, and tools; and

g. Leading the Village's privacy incident response and Privacy Incident Response Team, when required.

CONSEQUENCES OF NON-COMPLIANCE

a. Employees who fail to adhere to this policy may be subject to corrective action, including dismissal from employment, in accordance with the Labour Relations standard, or the specified terms outlined in their employment contract.

6. DEFINITIONS

In this Policy:

a. **Access and Privacy Program Administrator or APPA and Alternate** means the CAO or representative(s) appointed to coordinate activities supporting compliance and advancement of the PMP;

b. **Access to Information Request** means a request under *ATIA* for access to records for general or personal information in the custody or under the control of the Village;

c. **Automated System** means any system, software, or process that uses computation as a whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities.

d. **Bargaining Unit** means a group of employees who have a common interest and are represented by a single labour union, with an agreement with The Village in collective bargaining and other dealings with management;

e. **Conflict of Interest** means when a person or entity has a private or personal interest that could influence or compete with, or be perceived to influence or compete with, the objective exercise of the privacy incident investigation;

f. **Control** means The Village has the authority over the creation, use, distribution, retention, or disposition of the records;

g. **Custody** means records that are in The Village's possession and may include records supplied by a third party;

h. **Data Derived from Personal Information** means data created by data matching, and that identifies any individual whose personal information was used in the data matching;

i. **Data Matching** means linking personal information between two or more databases or other electronic sources of information;

j. **Disposition** means the formal process of removing records from custody when the retention period is met, by deletion or destruction, transfer to archival holdings, or transfer to another organization;

k. **Employee** means Village staff and any person who performs a service for the Village as an appointee, volunteer, or student, or under a contract or agency relationship with the Village as per *POPA*;

l. **Mosaic Effect** means a concept that illustrates how elements of information may be non-identifiable on their own but when combined could become personally identifiable;

m. **Non-Personal Data** means data, including data derived from personal information, that 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*;

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

- 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;
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual's age, gender identity, sex, sexual orientation, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;
- information about the individual's health and health care history, including information about the individual's physical or mental health;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and,
- the individual's personal views or opinions, except if they are about someone else.

o. **Personal Information Bank or PIB** means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. A PIB allows individuals to know the type of personal information the Village may have about them, how it is used, and the Village's authority for the collection;

p. **Privacy Incident** means an actual or suspected loss of, or unauthorized access to, use or disclosure of personal information or data derived from personal information;

q. **Privacy Impact Assessment or PIA** means an analytical process to help identify and address potential privacy risks with respect to a new, or substantial change to an existing administrative practice, program, project or service that will involve the collection, use or disclosure of personal information or data derived from personal information;

r. **Privacy Management Program or PMP** means a privacy management program established and implemented under POPA;

s. **Privacy Officer** means the person designated or identified to ensure the Village's compliance with *POPA*;

t. **Record** means any electronic record or other record in any form in which information is contained or stored, including information in any written, graphic, electronic, digital, photographic, audio, or other medium, but does not include any software or other mechanism used to store or produce the record;

u. **RROSH** means real risk of significant harm; and

v. **Synthetic Data** means artificial data created to maintain the structure and patterns of real data without being linked to any individual in the original data set.

ASSOCIATED AUTHORITY

This Policy is established in accordance with:

a. The Municipal Government Act (Alberta) which describes the responsibility of the Chief Administrative Officer to implement the policies and programs of the municipality;

b. Access to Information Act, SA 2024, Chapter A-1.4;

c. Protection of Privacy Act, SA 2024, Chapter P-28.5; and

APPENDIX 1 – PRIVACY INCIDENT RESPONSE PROTOCOL

PURPOSE

This Privacy Incident Response Protocol ("Protocol") outlines the steps that must be followed by all employees when a suspected or actual incident of privacy occurs. The Protocol allows the Village to identify, manage and respond to privacy incidents. The purpose of this Protocol is to:

a) Identify roles and responsibilities in responding to a privacy incident; and

b) Establish steps to be followed when responding to a privacy incident.

WHAT IS A PRIVACY INCIDENT?

A privacy incident means a loss of, or unauthorized access to, use or disclosure of personal information. The Village's definition of privacy incident is aligned with that of the Office of the Information and Privacy Commissioner ("OIPC") of Alberta.

This would include any event that results in personal information, data derived from personal information in the custody or under the control of The Village being collected, accessed, used, copied, modified, disclosed, or disposed of in an unauthorized manner, either deliberately or inadvertently.

KEY STEPS IN RESPONDING TO PRIVACY INCIDENTS

Initiate steps 1 through 3 as soon as a suspected or actual privacy incident has been identified. The Privacy Officer is accountable for all privacy incident activities.

1. Report

a. A suspected or actual privacy incident should immediately be reported by any employee to the Privacy Officer.

b. The public can fill out a *Privacy Incident Report (External)* form available at the Village Office.

2. Contain

Identify the scope of the privacy incident and contain it.

Will take and document immediate steps to contain the privacy incident and to secure the related records or information systems to prevent any further privacy incident from occurring. Containment should occur as soon as possible, and assistance may be sought from the Privacy Officer. Examples of containment activities include:

- Stopping the unauthorized practice;
- Recovering records;
- Shutting down the information system(s) that may have been breached;
- Revoking or changing computer access codes or correcting weaknesses in physical security; and
- Calling an unintended recipient to request written confirmation of the destruction of a document received in error.

Employees should be mindful not to destroy evidence that may be valuable in determining the cause and extent of the privacy incident, or that will allow the Village to take appropriate corrective action.

The affected area where the privacy incident occurred, should notify RCMP if the privacy incident involves theft or other criminal activity.

3. Investigate and Evaluation of Risk

The Privacy Officer will assign resources to investigate with the involvement of other parties, as necessary, and complete the following:

- Identify and analyze the events that led to the privacy incident;
- Obtain all relevant evidence;
- Document the privacy incident and containment activities;
- Inventory all personal information that was subject to the incident and determine the number of affected individuals;
- Determine the level of risk and level of harm.

The Privacy Officer will lead an objective investigation and address any real or perceived conflicts of interest. The Privacy Officer will determine and involve appropriate individuals and/or third-party investigative services, as required.
The Privacy Officer must evaluate whether the incident meets the threshold of a real risk of significant harm ("RROSH") to an individual.

As all incidents are unique, the Privacy Officer should exercise their judgment on each incident and consider the factors constituting RROSH under the *Ministerial Regulation.*

If any other relevant factors exist not included in the *Ministerial Regulation*, they should be considered during the evaluation.

If the privacy incident does not meet the threshold for RROSH, the privacy incident is tracked, responded to appropriately and recommendations are provided to prevent reoccurrence.

Privacy incident investigations that meet the threshold for RROSH will result in a *Privacy Incident Investigation Report*.

4. Notification

The outcome of the investigation and RROSH assessment determines whether notification is required under *POPA*.

If it is determined that the privacy incident meets the threshold for RROSH, the Privacy Officer is required to give notice, without unreasonable delay, to the affected individual(s), the OIPC and the Minister responsible for *POPA*. Prompt notification can help affected individual(s) mitigate the damage by taking steps to protect themselves.

Written notification occurs as set out in *POPA*.

Notification to affected individual(s), the OIPC and the Minister responsible for the Act must be in writing and include the information as prescribed in the *Ministerial Regulation*.

<u>Informing Village Council</u>

Where appropriate, Village Council (including CAO and Privacy Officer) will be provided information related to privacy incidents in order to support:

- The response activities;
- The implementation of recommendations; and

- Monitor and follow-up actions to prevent future privacy incidents.

Responsibilities related to informing and communicating privacy incidents to Village Privacy Officer and CAO and Village Council are set out below and in the Privacy Incident Response Procedure.

Individual Informing	Individual/Group to be Informed	When to Inform – Privacy Incidents
Employee, Access to Information and Investigations	Privacy Officer	All incidents
Privacy Officer	CAO, Privacy Officer	Real risk of significant harm assessment – This is initially based on information supplied in the *Privacy Incident Report Form.* Any change to the assessment through the investigation process will be communicated. • Incidents that *may* require notification to affected individuals; and • Incidents that *may* impact the financial, legal or reputational interests of the Village. **Will require assignment of point of contact to address questions from affected individual(s).*
	Village Council	• Incidents requiring notification to affected individual(s); • Incidents requiring notification to OIPC and the Minister; • Incidents requiring notification to third-party service providers; and • Incidents impacting the financial, legal or reputational interests of The Village.
Village Departments	Privacy Officer CAO	All incidents impacting their area of responsibility.

5. Prevent

Once the immediate steps have been taken to mitigate the risks associated with the privacy incident and notification has been completed (if required) the Privacy Officer will develop prevention strategies to mitigate against similar future privacy incidents.

Mitigation and prevention strategies should reflect the significance of the privacy incident and whether it was a systemic or isolated event. Strategies may include a review of:

- Physical safeguards (i.e. locks, alarms, security monitoring);
- Technical safeguards (i.e. restricting access, encryption on portable devices); and
- Administrative safeguards (i.e. policies, contractual clauses).

6. Follow-up

The Village tracks all privacy incidents across the organization and uses the information to identify trends in the types of privacy incidents occurring. This information can help identify underlying patterns with respect to personal information and data derived from personal information handling practices and may help prevent future privacy incidents.

The Privacy Officer will follow-up with the affected department(s) on the implementation of recommendations.

7. PRIVACY INCIDENT RESPONSE TEAM

Depending on the circumstances of the privacy incident, a Privacy Incident Response Team may be established by the Privacy Officer to respond to a privacy incident. Activities may include carrying out containment and assisting with notification to affected individual(s) to minimize any current, ongoing, or future privacy risks.

Membership of the Privacy Incident Response Team is determined by the Privacy Officer and varies depending on the context of the privacy incident. Where appropriate, the affected business unit(s) may identify subject matter experts as resources to support the Privacy Incident Response Team.

The Privacy Incident Response Team may include representation from the following:

Team Member	Role
Privacy Officer	Leads all activities and decisions by the Privacy Incident Response Team, including escalation. Manages the privacy incident response activities to contain, investigate, evaluate, document and make recommendations to mitigate future privacy incidents.
Law	Provides an assessment of the Village's legal position and legal advice pertaining to the privacy incident. This may include a review of legal, regulatory and contractual obligations. Reviews external communications to ensure that liability risk is managed.
Information Technology	Provides information system(s) and technology analysis related to privacy incident. Leads the containment activities as it relates to information systems and technologies.
CAO	Provides infrastructure and information asset security analysis related to the privacy incident. Leads security operations, monitoring, and response activities including cybersecurity incidents.
CAO	Provides personnel management and labour relations guidance related to the privacy incident. Leads the personnel management and labour relations activities including liaising with bargaining unit representatives, where required.

CAO	Provides support in the development of a communications plan, with tactics, timelines, and key messages for the purpose of preserving the Village's reputation, and trust with employees and the public.
Affected Department Unit(s)	Provides accurate incident details related to the privacy incident. Ensures that the department perspective is considered.

The *Privacy Incident Response Procedure* will include step-by-step instructions to help the Privacy Incident Response Team carry out its responsibilities.

8. ROLES AND RESPONSIBILITIES

Individuals	Roles	Responsibilities
All Employees	Employees need to be alert to the potential for personal information to be compromised, play a role in identifying, notifying, and containing a privacy incident.	• Report privacy incidents to their supervisor and/or Privacy Officer; • Notify RCMP if the privacy incident involves theft or other criminal activity; • Immediately undertake containment efforts; and • Assist with privacy incident investigations as required, including making factual corrections to privacy incident information.

Privacy Officer and/or CAO to Access Information and Investigations	The Privacy Officer is accountable for the Village's response to a privacy incident by ensuring that all key steps of the *Privacy Incident Response Protocol* are implemented. The Privacy Officer must address escalation decisions in a timely manner and determine the need to assemble a Privacy Incident Response Team. Response to a privacy incident may include working collaboratively with affected department(s) to contain, investigate, evaluate, document and make recommendations to mitigate future privacy risks.	• Intake and validate *Privacy Incident Report Form* information; • Investigate all suspected and actual privacy incidents; • Direct privacy incident response activities across affected departments(s); • Support containment of privacy incidents; • Conduct interviews; • Coordinate the collection of evidence and gathering of facts related to the privacy incident, and amend such information for accuracy, when required; • Investigate and evaluate the privacy incident and conduct a real risk of significant harm assessment; • Assemble and lead the Privacy Incident Response Team, when warranted; • Act as decision maker to involve third-party investigative services, as required; • Make escalation decisions related to privacy incidents;
		• Issue a *Privacy Incident Investigation Report*; • Notify affected individual(s), the OIPC and the Minister, as required; • Work with the OIPC, as required;

		• Issue recommendations to mitigate privacy incidents and follow-up on implementation of recommendations with affected business unit(s); • Close privacy incident response and debrief the Privacy Incident Response Team; • Collect, monitor, and assess all privacy incidents and identify trends and opportunities to prevent future privacy incidents;
CAO	Department(s) work collaboratively with the Privacy Officer to execute the key steps to responding to a privacy incident. Affected departments(s) have a role in mitigating recurring risks by implementing recommendations.	• Develop and implement a communication plan, as required; • Implement recommendations to mitigate privacy incident;
Village Council	Foster public trust and confidence in The Village.	• Maintain overall accountability for The Village's PMP; and • Inform the affected department (s) if escalation is required to assign a point of contact for inclusion on the *Letter of Notification* to address
Privacy Incident Response Team	Supports timely response to more complex privacy incidents.	• Assess, scope, and contain privacy incident; • Mitigate privacy risks; • Resource for affected department(s); and