TOWN OF MAGRATH
COUNCIL POLICY

TITLE: PRIVACY MANAGEMENT PROGRAM

RESOLUTION NUMBER: 2026-05-15	POLICY #: CP-030
	EFFECTIVE DATE: MAY 26, 2026
	SUPERSEDES:
	UP FOR REVIEW: 2030

PURPOSE

The purpose of this policy is to establish a comprehensive Privacy Management Program that ensures the Town of Magrath meets its obligations under applicable privacy legislation, including the Protection of Privacy Act (POPA). This policy provides a structured framework for the responsible collection, use, disclosure, and protection of personal and non-personal information. It is intended to promote accountability, transparency, and sound information governance practices while supporting the effective delivery of municipal services and maintaining public trust.

DEFINITIONS

Access: The ability or authority to view, retrieve, handle, or otherwise interact with Personal Information.

Administrative Safeguards: Policies, procedures, training, governance measures, and operational controls intended to protect Personal Information.

Agent: An entity authorized to act for or in place of another.

Annotation: A notation added to a record indicating that a correction was requested but not made, including the substance of the request.

Artificial Intelligence (AI): A system, model, or technology capable of generating content, analysis, recommendations, predictions, classifications, or decisions through automated or computational processes.

Automated System: A 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.

Complainant: An individual who submits a privacy complaint to the Town.

Consent: Voluntary agreement provided by an individual for the collection, use, or disclosure of their Personal Information, where such consent is required under applicable legislation.

Consistent Use: A use of Personal Information that has a reasonable and direct connection to the original purpose for which the information was collected and that an individual would reasonably expect.

Contact Information: Information to enable an individual or business to be contacted and includes the name, position or title, telephone number, address, email, or fax number of the individual or business.

Correction Request: A written request submitted by an individual seeking to correct or amend their personal information held by the Town.

Custody: The physical possession of a Record in addition to some right to deal with the Record and some responsibility for its care and protection. Custody normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security of the Record.

Data Derived from Personal Information: Data created from Personal Information through analysis, transformation, aggregation, matching, de-identification, or other processing activities, as authorized under applicable legislation.

Data Matching: The comparison, combination, or linking of Personal Information or records for the purpose of creating data derived from Personal Information.

Disclosure: The release, transfer, provision of, or granting access to Personal Information to any person, organization, or body outside of the Town or outside of authorized internal access permissions.

Disposition: The authorized destruction, deletion, transfer, or archival preservation of records in accordance with approved retention requirements.

Head: The Chief Administrative Officer (CAO), as defined under applicable legislation, who holds overall responsibility for the administration of the Town's privacy obligations.

Information Asset: Any record or data set, regardless of format, that is created, collected, stored, or used by the Town.

Information Sharing Agreement (ISA): A formal written agreement that establishes the terms, conditions, safeguards, responsibilities, and legal authority governing the sharing of Personal Information between the Town and another party.

Linkage: A mechanism by which a record is connected to additional information provided by an individual to ensure that future users are aware of a requested correction.

Non-Personal Data: Information that does not identify an individual and cannot reasonably be used to identify an individual, either alone or in combination with other information.

Personal Information: Recorded information about an identifiable individual, as defined under applicable privacy legislation.

Physical Safeguards: Physical measures intended to protect records, devices, systems, and facilities from unauthorized access, damage, theft, or loss.

POPA: The Protection of Privacy Act, as amended from time to time.

Privacy Breach: The unauthorized collection, use, disclosure, access, loss, or destruction of Personal Information in a manner contrary to POPA or municipal policy.

Privacy Commissioner: The Information and Privacy Commissioner of Alberta.

Privacy Complaint: A concern raised by an individual alleging that Personal Information has been collected, used, disclosed, accessed, retained, or managed in contravention of POPA or municipal privacy policies.

Privacy Impact Assessment (PIA): A Privacy Impact Assessment is a mandatory assessment that is conducted by a Public Body to determine if a current or proposed enactment, project, program or activity that involves personal information meets or will meet the privacy requirements of POPA.

Privacy Incident Response: The process that outlines steps in managing a known or suspected privacy breach.

Privacy Incident: Any event involving the unauthorized access, use, disclosure, loss, or destruction of personal information.

Privacy Management Program: A coordinated set of policies, procedures, and practices established to ensure compliance with privacy legislation and to manage privacy-related risks within the organization.

Privacy Officer: The individual designated by the Town to administer and maintain the Privacy Management Program and act as the Town's primary contact with the Information and Privacy Commissioner.

Privacy Training: Formal instruction provided to employees and other authorized individuals regarding privacy obligations, policies, procedures, and best practices.

Program Review: A formal or informal evaluation of the Privacy Management Program to assess effectiveness, compliance, and alignment with current requirements.

Public Body: Described in Section 1 (t) in the ATIA, including Local Public Bodies (as defined in Section 1 (n) of the ATIA).

Reasonable Security Safeguards: Administrative, physical, and technical safeguards implemented to protect information and data in a manner appropriate and proportionate to the associated risks and security classification level.

Records Retention Schedule: An approved framework that establishes minimum retention periods and disposition requirements for records and information assets.

Records: Information in any form: books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces Records (as defined in Section 1 (u) of the ATIA).

Re-identification: The process of linking Non-Personal Data to information that identifies or could reasonably identify an individual.

Security Classification: The categorization of information assets based on their sensitivity and the level of protection required.

Sensitive Personal Information: Recorded personal information with a higher risk of harm to individuals if the information is improperly collected, used or disclosed and may impact an individual's personal safety.

Significant Harm: Includes bodily harm, humiliation, damage to reputation or relationships, loss of employment or opportunities, identity theft, financial loss, negative impacts on credit or insurability, or other legal or financial harm.

Substantial Change: A significant modification to an existing administrative practice, program, project, or service that may materially affect the collection, use, disclosure, storage, access, retention, or protection of Personal Information.

Technological Safeguards: Technical and system-based security controls intended to protect Personal Information and information systems.

Use: Any internal handling, processing, consultation, analysis, or application of Personal Information by the Town.

POLICY STATEMENTS

1. This policy applies to all personal information, any data derived from personal information, and all non-personal data in the custody or under the control of the Town of Magrath. It further applies to all individuals acting on behalf of the Town, including council members, employees, officers, contractors, volunteers, and service providers, who are expected to handle information in accordance with this policy and its supporting procedures.

2. The Chief Administrative Officer, acting as the Head, is responsible for establishing, implementing, and maintaining the Town's Privacy Management Program. This includes the approval of privacy-related policies and procedures as administrative instruments. The CAO may delegate responsibilities in accordance with applicable legislation.

3. This policy is a Council policy establishing the governance framework for the Town's Privacy Management Program. All supporting policies, procedures, standards, guidelines, and related documents established under the Privacy Management Program, including those identified in Section 5 of this policy, are administrative policies and may be created, implemented, amended, maintained, or rescinded by Administration under the authority of the Chief Administrative Officer, unless otherwise required by legislation or directed by Council.

4. The Privacy Officer is responsible for administering and maintaining the Privacy Management Program on an ongoing basis. This includes monitoring compliance with established privacy policies, providing guidance to staff, and acting as the Town's primary point of contact with the Information and Privacy Commissioner.

5. The Town's Privacy Management Program consists of documented administrative policies and supporting procedures that address the Town's obligations under POPA, including but not limited to:

a. Roles & Accountability for Privacy
b. Privacy Training
c. Collection of Personal Information
d. Collection Notice and Consent
e. Access, Use, and Disclosure of Personal Information
f. Correction of Personal Information
g. Personal Information Classification System
h. Personal Information Safeguards
i. Personal Information Retention and Disposal
j. Privacy Impact Assessments
k. Creation, Use, and Disclosure of Non-Personal Data
l. Data Matching and Data Derived from Personal Information
m. Automated Systems and Artificial Intelligence
n. Privacy Incident and Breach Response
o. Privacy Complaints Handling
p. Program Review & Updates

6. The Privacy Management Program will be proportionate to the volume, sensitivity, and complexity of the information managed by the Town. Programs or systems involving sensitive personal information, automated decision-making, or significant data sharing will be subject to enhanced safeguards and oversight to address elevated risks.

7. Any person may request access to the Town's Privacy Management Program. The Town will provide access, either by supplying a copy or directing the requester to where the program can be accessed, within 30 business days. The Town may withhold technical or security-sensitive details where disclosure could reasonably compromise information security, in accordance with applicable legislation.

8. The Town will periodically review its privacy policies and procedures, the effectiveness of employee training, and the privacy risks associated with its programs and systems. Reviews may be undertaken in response to legislative or regulatory changes, significant modifications to programs or systems, privacy incidents or complaints, or findings arising from audits or formal reviews.

9. Compliance with the Privacy Management Program is mandatory. Failure to comply may increase the Town's exposure to legal, operational, and reputational risks and may result in corrective administrative action in accordance with municipal policies.