

Policy



Medicine Hat

Title: Privacy Management		Number: 0193-2026
Reference: Administrative Committee April 8, 2026 Administrative and Legislative Review and Government Relations Committee April 14, 2026	Adopted by City Council: May 4, 2026	
	City Clerk	City Manager
Supersedes:		
Prepared by: City Clerk Department		

STATEMENT

The City of Medicine Hat is committed to protecting the privacy of individuals whose information is collected, used, disclosed, or stored by the City by establishing a Privacy Management Program to be implemented using a phased, risk-based approach, recognizing that some components will be developed over time.

PURPOSE

This policy will establish the governance framework and define components for the City's Privacy Management Program to promote consistent, secure, and lawful handling of Individual-Related Data and ensure the City meets its legislated obligations.

1. DEFINITIONS

- 1.1 **ATIA** means the *Access to Information Act*, RSA 2024, c. A-1.4.
- 1.2 **ATIA-R** means the *Access to Information Act Regulation*, Alberta Regulation 133/2025.
- 1.3 **Automated System** means a system that contains Personal Information used by the City to inform decision-making.
- 1.4 **City** means the municipal corporation of the City of Medicine Hat.
- 1.5 **City Manager** means the person appointed by Council to the position of Chief Administrative Officer or their delegate.
- 1.6 **Control** means the City's authority related to the creation, use, distribution, retention or disposition of Individual-Related Data.

- 1.7 **Consent** means an individual's voluntary and informed agreement to the collection, use, or disclosure of their personal information, provided in a manner permitted under Privacy Legislation.
- 1.8 **Custody** means Individual-Related Data that is in the City's possession and may include Individual-Related Data that is supplied by a third party.
- 1.9 **Derived Data** means data created by Data Matching that identifies or presents a reasonable risk of identifying or reidentifying, an individual whose Personal Information was used in the Data Matching.
- 1.10 **Data Matching** means linking Personal Information between two or more databases or other electronic sources of information.
- 1.11 **Individual-Related Data** means Personal Information, Derived Data, and Non-Personal Data collectively.
- 1.12 **Non-Personal Data** means data, including Derived Data, that has been generated, modified or anonymized so that it does not identify any individual.
- 1.13 **POPA** means the *Protection of Privacy Act*, RSA 2024, c.P-28.5
- 1.14 **POP-R** means the *Protection of Privacy Regulation*, Alberta Regulation 132/2025
- 1.15 **POP-MR** means the *Protection of Privacy (Ministerial) Regulation*, Alberta Regulation 143/2025
- 1.16 **Personal Information** means information about an identifiable individual as defined in POPA.
- 1.17 **Personal Information Bank** means a collection of Personal Information as defined in POPA.
- 1.18 **Privacy Incident** means actual or suspected loss, unauthorized access, or unauthorized disclosure of Personal Information.
- 1.19 **Privacy Impact Assessment (PIA)** means a documented assessment of privacy risks associated with a program, system, or initiative.
- 1.20 **Privacy Management Program** means a privacy management program established and implemented pursuant to section 25 of POPA.
- 1.21 **Provincial Privacy Legislation** means ATIA, ATIA-R, POPA, POP-R, and POP-MR collectively.

2. AUTHORITY

- 2.1 Pursuant to Section 201 of the *Municipal Government Act* (Alberta), Council is responsible for developing and evaluating the policies of the City. Pursuant to Section 207 of the *Municipal Government Act* (Alberta), the City Manager is responsible for ensuring that the policies of the City are implemented.

Policy 0193-2026 – Privacy Management		
Approved by:	City Council - May 4, 2026	Page 3 of 5

- 2.2 This policy guides the City's Privacy Management Program pursuant to Provincial Privacy Legislation.
- 2.3 If any provision of this policy conflicts with any provision of Provincial Privacy Legislation, the provision of Provincial Privacy Legislation prevails.

3. APPLICABILITY

- 3.1 This policy applies to all Individual-Related Data in the Custody and Control of the City.
- 3.2 This policy applies to any person who handles or has access to information set out in section 3.1.

4. PRINCIPLES

- 4.1 Without limiting the generality of the City's obligations under Provincial Privacy Legislation, the City acknowledges that the privacy and confidentiality of Individual-Related Data is important and commits to treating all Individual-Related Data with respect pursuant to Provincial Privacy Legislation.
- 4.2 The City will establish and maintain the following Privacy Management Program components. Where components are not yet fully developed, the City will implement the components in phases.
 - (a) Collection, Consent, and Notice
 - (i) Collect only what is authorized by law and necessary to support the City's common or integrated operational programs, services or activities.
 - (ii) Obtain meaningful Consent of the individual (or the parent or legal guardian for any individual who is unable to provide meaningful Consent on their own), except where POPA permits or requires otherwise.
 - (iii) Provide clear and understandable notice at or before the time of collection as required by POPA.
 - (iv) Develop, maintain, and publish a directory that lists the City's Personal Information Banks.
 - (b) Use and Disclosure

Use and disclose Individual-Related Data only in circumstances permitted by Privacy Legislation.
 - (c) Access, Accuracy, and Correction of Personal Information

Ensure accuracy of Personal Information in the Custody and Control of the City and allow individuals to request access to Personal Information or a correction to Personal Information.

- (d) **Retention and Disposition of Individual-Related Data**
Ensure that all Individual-Related Data is retained and disposed of in accordance with established records management procedures and Provincial Privacy Legislation.
- (e) **Protection of Personal Information**
Establish security measures to protect Personal Information from unauthorized access, collection, use, disclosure, alteration or destruction through administrative, physical, and technical controls, including a classification system based on sensitivity and risk.
- (f) **Third Parties and Contracts**
Ensure all contracts entered into by the City that may involve the collection, use, or disclosure of Personal Information in the performance of the contract, include a requirement for reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.
- (g) **Privacy Impact Assessments**
Conduct Privacy Impact Assessments with a level of detail commensurate with the complexity for new or significantly modified practices, programs, projects, or services that will involve the collection, use, or disclosure of Personal Information.
- (h) **Privacy Incident Response**
Maintain a Privacy Incident Response Protocol that describes the roles and responsibilities for managing actual or suspected privacy incidents.
- (i) **Automated System Transparency**
If an Automated System uses Personal Information, provide the required notice to individuals and ensure human oversight.
- (j) **Derived Data, Non-Personal Data, and Data Matching**
 - (i) Ensure that Derived Data is managed in a manner consistent with the original authority, purpose, and privacy requirements associated with the Personal Information from which it was derived and is treated as Personal Information where there is a reasonable possibility of identification or re-identification.
 - (ii) Ensure that Non-Personal Data is managed and governed in a manner that prevents identification or re-identification of individuals, including through the application of reasonable technical, administrative, and contractual controls, particularly where data is combined with other datasets or shared internally or externally.
 - (iii) Ensure that Data Matching and the use of Non-Personal Data are undertaken only where legally authorized, necessary, and

Policy 0193-2026 – Privacy Management		
Approved by:	City Council - May 4, 2026	Page 5 of 5

proportionate, with scope limited to relevant data elements and reasonable measures in place to prevent the identification or re-identification of individuals, including when data is combined with other datasets or shared internally or externally.

(k) Training and Awareness

Ensure that all individuals identified in section 3.2 receive access and privacy training as applicable to their role.

- 4.3 Components of the Privacy Management Program will be reviewed annually to ensure compliance and risk mitigation.
- 4.4 A public-facing summary of components of the Privacy Management Program will be published on the City's website and updated as components are established or amended, as required by POPA.

5. RESPONSIBILITIES

5.1 Council

- (a) Receive, review and approve this policy and any recommended amendments.

5.2 City Manager

- (a) Implement this policy, which includes ensuring that an appropriate procedure and Privacy Management Program components are established.

Procedure



Medicine Hat

Title: Privacy Management		Number: 0193-2026
Approved by the Administrative Committee: July 22, 2026		Supersedes:
City Clerk	City Manager	
Prepared by: City Clerk		

1. DEFINITIONS

All defined terms in Privacy Management Policy 0193-2026 ("Policy 0193-2026") apply to this procedure wherever used. For the purposes of interpretation of this procedure, the term Privacy Management Program is meant to be inclusive of Policy 0193-2026 and this procedure.

- 1.01 **Head** means the City Clerk, as appointed by the City's Administrative Organization Bylaw 4662 pursuant to Provincial Privacy Legislation.
- 1.02 **Privacy Officer** means the position designated in writing by the Head that is responsible for overseeing the Privacy Management Program and ensuring the City remains operationally compliant with Provincial Privacy Legislation.

2. RESPONSIBILITIES

2.01 Administrative Committee

- (a) Receive, review and approve this procedure and any recommended amendments.

2.02 Executive Leadership Team

- (a) Ensure reasonable efforts are made to provide access to Personal Information and records.
- (b) Communicate expectations for Employee conduct and accountability related to the Privacy Management Program.

2.03 Head

- (a) Designate, in writing, the position of Privacy Officer.

2.04 Privacy Officer

- (a) Monitor and ensure compliance with Provincial Privacy Legislation.
- (b) Develop, maintain, and annually review the components of the Privacy Management Program.
- (c) Take appropriate action in response to formal access to information requests submitted by members of the public pursuant to Provincial Privacy Legislation.
- (d) In consultation with the Head, communicate with the Office of the Information and Privacy Commissioner of Alberta, including coordinating any negotiations, mediations, inquiries, and investigations on behalf of the City.
- (e) Lead the City's training on Provincial Privacy Legislation and the Privacy Management Program.
- (f) In consultation with the Head, Lead the City's response to Privacy Incidents.

2.05 Department Directors

- (a) Appoint at least one privacy contact and an alternate for the department (or each business unit, if deemed operationally preferable) to:
 - (1) serve as point of contact for the Privacy Officer to ensure that access to information requests are processed effectively;
 - (2) ensure that information that can be routinely disclosed is identified; and
 - (3) ensure that privacy protection measures are implemented.
- (b) Ensure all employees receive access and privacy training as applicable for their role.
- (c) Ensure all employees, services, programs, and systems are compliant with the Privacy Management Program.

2.06 Department Privacy Contact

- (a) Attend training specified by the Privacy Management Program and, in consultation with the Privacy Officer, provide corresponding advice and guidance to their department or business unit regarding compliance with Provincial Privacy Legislation.
- (b) Seek guidance from the Privacy Officer regarding new or complex situations involving Personal Information.

- (c) Lead the department or business unit response to the Privacy Officer, which includes coordinating the search for, identifying and retrieving records responsive to access to information requests.
- (d) Ensure that the department or business unit perspective is documented in any recommendation on a response to an access to information request.
- (e) Facilitate the completion and maintenance of department or business unit Privacy Impact Assessments (PIAs).
- (f) Ensure Personal Information Banks are created or modified on behalf of the department or business unit.
- (g) Support the department or business unit to protect Personal Information, report any suspected or actual Privacy Incidents or potential breaches, assist with audits and privacy incident investigations, and assist with implementation of corrective actions.
- (h) Conduct regular reviews to ensure compliance with the Privacy Management Program and report non-compliance concerns to the department director or Privacy Officer when issues arise.

2.07 Employees

- (a) Understand their roles and responsibilities under the Privacy Legislation and adhere to the City's Privacy Management Program.
- (b) Collect, use, and disclose Personal Information only as authorized by Provincial Privacy Legislation.
- (c) Use reasonable security safeguard measures to protect and manage Personal Information in the City's Custody or under its Control against risks of unauthorized access, collection, use, disclosure or destruction.
- (d) Make every reasonable effort to provide appropriate access to Personal Information in the City's Custody or under its Control pursuant to Provincial Privacy Legislation.
- (e) Respond to requests from the Privacy Officer pursuant to formal access to information requests in a timely manner by searching for, documenting, and producing all responsive records.
- (f) Report any suspected or actual withholding of records, failure to produce responsive records, or any other conduct that may be inconsistent with Provincial Privacy Legislation or the Privacy Management Program to the Department Privacy Contact or the Privacy Officer.
- (g) Participate in access and privacy training to understand appropriate collection, use, protection, management, disclosure, correction, and

disposition of Personal Information as required by their job duties and responsibilities.

- (h) Participate in PIAs 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.
- (i) Report any Privacy Incidents to the Privacy Officer and take reasonable action to limit the scope and impact of any Privacy Incident where possible.
- (j) Review privacy recommendations and implement the recommended privacy risk mitigation strategies where possible.
- (k) Make factual corrections to Personal Information without a formal request pursuant to Provincial Privacy Legislation when directly requested by the individual to whom the Personal Information relates if it is practical and expedites public business.

3. PROCEDURES

3.01 Specific procedures, processes, practices, protocols, etc. are, or will be, contained within components of the Privacy Management Program. Those components will include, but may not be limited to:

- (a) Collection, Consent, and Notice
- (b) Use and Disclosure
- (c) Access, Accuracy, and Correction of Personal Information
- (d) Retention and Disposition of Personal Information
- (e) Non-Personal Data (anonymized, ee-identified, and synthetic data)
- (f) Protection of Personal Information
- (g) Third Parties and Contracts
- (h) Privacy Impact Assessments
- (i) Privacy Incident Response
- (j) Data Derived from Personal Information, and Non-Personal Data

3.02 Components of the Privacy Management Program are developed and maintained by the Privacy Officer and will be implemented in phases.