CITY OF MEDICINE HAT

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		**Supersedes:**
	City Clerk	**City Manager**	
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.

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

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.