



TOWN OF NANTON PRIVACY MANAGEMENT FRAMEWORK



Table of Contents



PART I

Privacy Governance

- 1.1 Our Privacy Commitment
- 1.2 Privacy Governance



PART II

Privacy Program Components

- 2.1 Legislation and Policies
- 2.2 Collection, Retention and Disposition of Personal Information
- 2.3 Personal Information Inventory
- 2.4 Privacy Impact Assessments
- 2.5 Information Security and Safeguards
- 2.6 Service Provider and Contractor Management



PART III

Building a Privacy-Aware Organization

- 3.1 Education and Awareness
- 3.2 Continuous Improvement

PRIVACY COMMITMENT



The Town of Nanton recognizes that privacy protection is a shared responsibility. Council, Administration, employees, contractors, and service providers all play an important role in ensuring personal information is collected, used, disclosed, retained, and protected in accordance with applicable legislation.

Through its Privacy Management Program, the Town is committed to:

- ✓ Protecting personal information throughout its lifecycle.
- ✓ Maintaining compliance with POPA, ATIA, and related legislation.
- ✓ Building privacy considerations into municipal programs, services, technologies, and decision-making processes.
- ✓ Providing transparency regarding how personal information is managed.
- ✓ Promoting accountability and responsible information handling practices.
- ✓ Continuously improving privacy controls and safeguards.

GUIDING PRINCIPLES



Privacy Governance





Legislation and Policies



Legislation



On June 11, 2025, Alberta's Freedom of Information and Protection of Privacy Act (FOIP) was repealed and replaced by two separate statutes: the **Access to Information Act (ATIA)** and the **Protection of Privacy Act (POPA)**.



The **Access to Information Act** establishes a right of access to records in the custody or under the control of public bodies, subject to limited and specific exceptions. The Act also provides individuals with a right to access their own personal information, request corrections to personal information, and seek an independent review of decisions made by a public body through the Office of the Information and Privacy Commissioner (OIPC).



The **Protection of Privacy Act** establishes rules governing the collection, use, disclosure, retention, protection, and disposal of personal information by public bodies. POPA also requires public bodies to implement and maintain a Privacy Management Program appropriate to the volume and sensitivity of the personal information in their custody or under their control.



Privacy Management Program

An overarching framework that establishes privacy practices, assigns responsibilities, and ensures compliance with legislation. It guides, supports, and is operationalized through governance policies and operational procedures.



Governance Policies



• Access, Privacy & Routine Disclosure Policy



• Information Security & Acceptable Technology Use Policy



• AI & Automated Systems Governance Policy



• Information Sharing & Service Provider Standard



• Surveillance Policy



Operational Procedures



• Privacy Breach & Incident Response Procedure



• Privacy Impact Assessment and Risk Management Procedure



• Records Retention & Secure Destruction Procedure



Collection, Retention and Disposition of Personal Information



Every day, the Town of Nanton collects and manages personal information to deliver municipal services, support decision-making, and serve the community effectively. Whether processing utility accounts, administering recreation programs, responding to concerns, managing permits, or supporting municipal operations, the Town is committed to handling personal information responsibly and respectfully.



The Town collects only the personal information necessary to carry out authorized municipal programs, services, and activities, and ensures individuals are informed about why their information is being collected and how it will be used.



Protecting privacy extends beyond collection. The Town manages personal information throughout its entire lifecycle—from the moment it is collected until it is securely destroyed or preserved in accordance with legal, operational, and historical requirements. Records are retained only as long as necessary to meet legislative, business, financial, and archival obligations and are disposed of in a secure and responsible manner when no longer required.



Through strong records management practices, clear retention requirements, and appropriate safeguards, the Town works to ensure personal information remains accurate, secure, accessible when needed, and protected throughout its lifecycle.





Personal Information Inventory



The Town is developing and maintaining a comprehensive inventory of **personal information** collected, used, disclosed, stored, and retained across municipal departments.

This inventory helps the Town:



Understand
what information
it holds.



Identify
privacy risks.



Support
access requests and
correction requests.



Meet
legislative
requirements.



Improve
accountability and
transparency.



By maintaining an accurate and up-to-date inventory, the Town ensures personal information is managed **responsibly, securely, and in compliance** with privacy legislation.





Privacy Impact Assessments



Privacy Impact Assessments (PIAs) are an important risk management tool used to identify, assess, and mitigate privacy risks before implementing new initiatives or significant changes involving personal information. A PIA is a structured review that examines how personal information will be collected, used, disclosed, stored, protected, and disposed of, while identifying potential privacy, security, operational, and compliance risks associated with a proposed program, service, technology, system, or process.



Under the **Protection of Privacy Act (POPA)**, Privacy Impact Assessments are required for applicable initiatives implemented on or after June 11, 2025, when the legislation came into force.

While existing programs and services established prior to this date may not require a PIA, the Town may undertake assessments where significant changes occur, or privacy risks warrant further review.



The Town utilizes Privacy Impact Assessments to evaluate privacy risks associated with:



-  • New programs and services;
-  • New technologies and software systems;
-  • Artificial intelligence and automated systems;
-  • Information-sharing arrangements;
-  • Surveillance and monitoring technologies; and
-  • Other initiatives involving personal information.



Information Security and Safeguards



Protecting personal information requires more than policies and procedures—it requires a coordinated approach that integrates privacy and security into daily municipal operations. The Town of Nanton is committed to implementing administrative, physical, and technical safeguards designed to protect personal information from unauthorized access, use, disclosure, alteration, loss, theft, or destruction.



These safeguards help ensure personal information remains secure throughout its lifecycle and support the Town's ability to maintain public trust, meet legislative requirements, and reduce privacy and cybersecurity risks.

SAFEGUARDS IMPLEMENTED BY THE TOWN INCLUDE:



- Employee confidentiality and information handling requirements;



- Secure storage and protection of physical and electronic records;



- Access controls and user permissions based on business need;



- Cybersecurity measures and technology protections;



- Records management and retention practices;



- Monitoring, auditing, and risk management activities; and



- Privacy and security requirements for contractors and service providers.



Service Provider and Contractor Management



The Town of Nanton recognizes that contractors, consultants, software vendors, cloud service providers, and other third-party service providers may collect, access, use, store, disclose, or manage personal information on behalf of the municipality.

While these services may be provided by external organizations, the Town remains accountable for the protection of personal information entrusted to it.



To support compliance with legislative requirements and reduce privacy risks, the Town incorporates privacy, security, confidentiality, breach reporting, and information management requirements into applicable agreements, contracts, and information-sharing arrangements.

These requirements help ensure third parties understand their responsibilities and maintain safeguards appropriate to the information they handle.



The Town's Privacy Management Program establishes standards for the selection, oversight, and management of service providers to promote responsible information handling.

These standards support compliance with privacy legislation and protect personal information throughout the duration of the relationship.

KEY EXPECTATIONS FOR SERVICE PROVIDERS AND CONTRACTORS



CONTRACT REQUIREMENTS

Privacy, security, confidentiality, and breach reporting obligations are built into contracts.



DUE DILIGENCE

Service providers are assessed for their ability to protect personal information.



APPROPRIATE SAFEGUARDS

Providers must implement and maintain safeguards appropriate to the information they handle.



BREACH REPORTING

Providers must promptly inform the Town of any privacy breach or security incident.



ONGOING OVERSIGHT

The Town monitors and reviews service providers to ensure ongoing compliance.



RETURN OR DISPOSAL

Personal information must be returned or securely destroyed at the end of the contract.



Education and Awareness



Building a strong culture of privacy awareness is a key component of the Town's Privacy Management Program. Protecting personal information is not solely the responsibility of one department or individual—it requires awareness, understanding, and accountability across the organization and among those who handle information on the Town's behalf.



The Town's privacy education and awareness program is intended to support Council, employees, volunteers, contractors, service providers, third-party partners, and other connected organizations that collect, access, use, disclose, or manage information in support of municipal operations. The objective is to ensure privacy considerations become part of everyday decision-making, service delivery, and information management practices.



The Town is developing a privacy education program that includes:



Employee privacy awareness training;



Council education and governance awareness;



Department-specific guidance materials;



Privacy breach response training;



Access to information guidance;



Privacy resources for contractors, service providers, and third-party partners; and



Ongoing privacy communications and resources.



Improving Privacy Practices

CONTINUOUS IMPROVEMENT



Privacy management is an ongoing commitment that evolves alongside legislation, technology, and municipal operations. The Town of Nanton will regularly review and enhance its Privacy Management Program to ensure it remains effective, relevant, and aligned with legislative requirements and industry best practices.



Reviews may be undertaken in response to legislative amendments, new technologies, operational changes, emerging privacy and cybersecurity risks, audit findings, privacy incidents, lessons learned, and opportunities for improvement identified through ongoing monitoring and assessment activities.

REVIEWS MAY BE TRIGGERED BY:



Legislative amendments



New technologies



Operational changes



Emerging privacy and cybersecurity risks



Audit findings



Privacy incidents



Lessons learned



Opportunities for improvement



By continually evaluating and strengthening its privacy practices, the Town seeks to **reduce risk, enhance accountability, improve service delivery, and maintain the confidence** of residents, employees, and stakeholders in the responsible management of personal information.



NANTON

EST



1903

Questions?



Email

communications@nanton.ca



Our Website

www.nanton.ca