



Town of Stavelly – Policy #02-09
Policy Area: Legislative
Municipal Privacy Management Program Policy

POLICY TITLE: MUNICIPAL PRIVACY MANAGEMENT PROGRAM POLICY

Date Approved by Council: May 25, 2026

Resolution No: 26-114

Last Review Date:

Replaces: N/A

Next Review Date: Every 3 years, at a minimum

Policy Statement:

The purpose of this Privacy Management Program (PMP) is to ensure that the Town of Stavelly (the “Town”) complies with the:

- Protection of Privacy Act (“POPA”); and
- Access to Information Act (“ATIA”)

respecting the collection, use, disclosure, retention, security, correction, and destruction of personal information.

This Policy establishes a comprehensive framework of policies, procedures, safeguards, and accountability measures to demonstrate due diligence, transparency, and continuous improvement in accordance with Alberta legislation and guidance issued by the Office of the Information and Privacy Commissioner of Alberta (“OIPC”).

Definitions:

Personal Information

For the purpose of this policy, “Personal Information” means recorded information about an identifiable individual, including information that identifies an individual directly or indirectly.

Personal information includes, but is not limited to:

- name, address, telephone number, email address, or identifying numbers;
- demographic information;
- employment, educational, financial, or criminal history;
- opinions or views of or about an individual;



Town of Stavely – Policy #02-09

Policy Area: Legislative

Municipal Privacy Management Program Policy

- health information;
- biometric information;
- and any other information reasonably capable of identifying an individual.

Personal information does not include information relating to an individual acting in a business, professional, or official capacity unless that information reveals something personal about the individual.

Purpose / Guidelines:

This policy applies to:

- all Town employees, contractors, volunteers, elected officials, and service providers;
- all personal information in the custody or control of the Town;
- and all records regardless of format, including paper, electronic, audio, video, and metadata.

LEGISLATIVE AUTHORITY

This policy is established pursuant to:

- Protection of Privacy Act;
- Access to Information Act;
- applicable regulations;
- and guidance or orders issued by the Office of the Information and Privacy Commissioner of Alberta.

GOVERNANCE AND ACCOUNTABILITY

Head of the Public Body

The Chief Administrative Officer (CAO) is the Head of the Public Body and is ultimately responsible for compliance with ATIA and POPA.

Privacy Officer

The Town shall designate a Privacy Officer responsible for:

- administering privacy compliance;
- responding to access requests;
- coordinating breach response procedures;
- maintaining records relating to privacy matters;



Town of Stavely – Policy #02-09
Policy Area: Legislative
Municipal Privacy Management Program Policy

- coordinating Privacy Impact Assessments (PIAs);
- and acting as liaison with the OIPC.

The Town shall maintain current contact information for the Privacy Officer.

Employees and Contractors

All employees, contractors, and volunteers shall:

- comply with this policy;
- protect personal information in their custody or control;
- and immediately report suspected or confirmed privacy breaches.

CORE PRIVACY PRINCIPLES

The Town adopts the following privacy principles:

- **Authority and Necessity**
Personal information shall only be collected where authorized and necessary.
- **Purpose Limitation**
Personal information shall only be used for the purpose for which it was collected or for a consistent purpose authorized by legislation.
- **Data Minimization**
Only the minimum amount of personal information required shall be collected and retained.
- **Accuracy**
Reasonable steps shall be taken to ensure information is accurate and current.
- **Security and Safeguards**
Personal information shall be protected against unauthorized access, disclosure, loss, or destruction.
- **Transparency and Accountability**
Privacy practices shall be documented, reviewable, and auditable.

COLLECTION OF PERSONAL INFORMATION

The Town shall:

- collect personal information only where authorized by legislation;
- limit collection to information necessary for municipal operations;
- and provide collection notices where required.



Town of Stavely – Policy #02-09
Policy Area: Legislative
Municipal Privacy Management Program Policy

Collection notices shall identify:

- the authority for collection;
- the purpose of collection;
- and contact information for the Privacy Officer.

USE AND DISCLOSURE OF PERSONAL INFORMATION

Personal information may only be:

- used for the purpose for which it was collected;
- used for a consistent purpose;
- or disclosed where authorized or required by legislation.

Unauthorized disclosure of personal information is prohibited.

PRIVACY IMPACT ASSESSMENTS (PIAs)
--

A Privacy Impact Assessment shall be completed where:

- new programs, systems, or technologies involve personal information;
- data matching activities are proposed;
- or automated systems or artificial intelligence tools process personal information.

The Privacy Officer shall review all PIAs prior to implementation.

PERSONAL INFORMATION BANKS

The Town shall maintain a directory of Personal Information Banks (PIBs) identifying:

- categories of personal information;
- purposes for collection;
- retention periods;
- and applicable safeguards.

The PIB inventory shall be reviewed periodically and updated as required.

RECORDS MANAGEMENT

The Town shall maintain records management practices sufficient to:

- retrieve records within legislated timelines;
- protect records from unauthorized access;
- and support legal retention requirements.



Town of Stavely – Policy #02-09
Policy Area: Legislative
Municipal Privacy Management Program Policy

SECURITY SAFEGUARDS

The Town shall implement reasonable administrative, physical, and technical safeguards to protect personal information including:

- password protection;
- access controls;
- secure storage;
- employee training;
- and secure destruction procedures.

STAFF TRAINING

Employees handling personal information shall receive privacy and access to information training appropriate to their role.

Training may include:

- POPA and ATIA awareness;
- records handling;
- breach reporting procedures;
- cybersecurity awareness;
- and role-specific privacy responsibilities.

CORRECTION OF PERSONAL INFORMATION

Individuals may request correction of their personal information in accordance with POPA.

The Town shall:

- acknowledge correction requests;
- investigate the request;
- and either correct the information or annotate the record where correction is refused.

PRIVACY BREACH RESPONSE

The Town shall maintain a documented Privacy Breach Response Procedure.

All suspected or confirmed privacy breaches shall be immediately reported to the Privacy Officer.



Town of Stavely – Policy #02-09
Policy Area: Legislative
Municipal Privacy Management Program Policy

The Town shall:

- contain breaches;
- assess risks;
- notify affected individuals where required;
- notify the OIPC where required;
- document all breaches;
- and implement corrective actions.

SERVICE PROVIDERS

The Town remains responsible for personal information handled by contractors and service providers.

Contracts involving personal information shall include provisions respecting:

- confidentiality;
- safeguards;
- breach notification;
- retention;
- destruction;
- and compliance with applicable legislation.

AUTOMATED SYSTEMS AND ARTIFICIAL INTELLIGENCE
--

Where automated systems or artificial intelligence process personal information, the Town shall:

- complete a Privacy Impact Assessment;
- provide notice where required;
- maintain safeguards respecting derived data;
- and establish procedures allowing individuals to question or contest automated decisions.

PRIVACY COMPLAINTS

Individuals may submit privacy complaints to the Privacy Officer.



Town of Stavely – Policy #02-09
Policy Area: Legislative
Municipal Privacy Management Program Policy

The Town shall:

- acknowledge complaints within five (5) business days;
- investigate complaints;
- provide a written response within thirty (30) business days where reasonably practicable;
- and advise complainants of their right to contact the OIPC.

ACCESS TO INFORMATION REQUESTS

Requests for access to records shall be processed in accordance with ATIA.

The Town shall designate an Access to Information Coordinator responsible for:

- receiving requests;
- coordinating responses;
- tracking timelines;
- and ensuring compliance with legislative requirements.

Department Instructions:

All Town departments shall ensure compliance with:

- Protection of Privacy Act (“POPA”);
- Access to Information Act (“ATIA”);
- and Town of Stavely Policy No. 02-09 – Municipal Privacy Management Program.

Department Heads shall:

- identify areas where personal information is collected or maintained;
- ensure staff receive privacy-related training;
- immediately report suspected privacy breaches to the Privacy Officer;
- ensure records containing personal information are securely stored;
- ensure forms collecting personal information contain appropriate privacy notices;
- cooperate with access to information requests and Privacy Impact Assessments;
- and ensure contractors handling municipal information comply with municipal privacy requirements.

Employee Responsibilities

All employees, contractors, volunteers, and elected officials shall:

- protect personal information from unauthorized access or disclosure;
- access personal information only where required for their duties;
- immediately report suspected privacy breaches;
- comply with records retention and destruction procedures;
- and complete mandatory privacy training when required.



Town of Stavely – Policy #02-09
Policy Area: Legislative
Municipal Privacy Management Program Policy

Records and Information Handling

Departments shall:

- maintain records in accordance with municipal retention schedules;
- avoid unnecessary collection of personal information;
- ensure passwords and access credentials remain secure;
- and ensure paper and electronic records are protected from unauthorized access.

Privacy Breach Reporting

Any suspected or confirmed privacy breach shall immediately be reported to:

- the Chief Administrative Officer; or
- the designated Privacy Officer.

Departments shall cooperate fully in breach investigations and corrective actions.

Privacy Impact Assessments (PIAs)

Departments proposing:

- new software,
- surveillance systems,
- automated decision-making systems,
- AI tools,
- or new programs involving personal information

must consult Administration prior to implementation to determine whether a Privacy Impact Assessment is required.