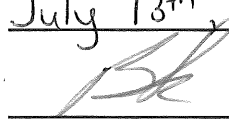


PRIVACY MANAGEMENT PROGRAM:

- **GENERAL PROGRAM POLICY**
- PRIVACY POLICY
- ACCESS POLICY
- SECURITY POLICY

DRAFT DATE: July 13th, 2026

APPROVED: 

Carmie M. Callin

Table of Contents

GENERAL PROGRAM POLICY

I.	PURPOSE	3
II.	SCOPE	3
III.	GOALS AND PRINCIPLES	3
IV.	ROLES AND RESPONSIBILITIES	5
V.	QUALITY CONTROLS AND ASSURANCE.....	7
VI.	TERMS AND DEFINITIONS.....	9

TOWN OF TROCHU – POLICY

POLICY # 2026-07-13-01

POLICY NAME: Trochu Privacy Management Program: General Program Policy

I. PURPOSE

The *Alberta Access to Information Act* (“ATIA”) ensures individual right of access to information and protects the personal information of the public, and employees of public bodies operating in Alberta. The Town of Trochu (“Trochu”) is bound by the requirements of the *Protection of Privacy Act* (“POPA”) and collects, uses, and discloses personal information in accordance with its provisions.

Trochu has established a comprehensive Privacy Management Program comprised of policies, procedures, and additional information such as forms and education/training materials. This policy establishes the principles and processes for managing Trochu information in compliance with ATIA and POPA and is supported by policies and procedures related to privacy, access and security.

II. SCOPE

This policy applies to:

1. Trochu employees, including directors, officers, contractors, students, and volunteers providing services on behalf of Trochu;
2. All recorded information, in whatever form or medium (paper, digital, audio-visual, graphic) created or received in the course of carrying out Trochu’s mandated functions and activities; and
3. All facilities and equipment required to collect, manipulate, transport, transmit, or keep Trochu information.

III. GOALS AND PRINCIPLES

Trochu is committed to providing full informational accountability and to protecting the privacy of individual citizens and its employees. To that end, Trochu has implemented a privacy and access program to meet the following goals and principles:

A. PROGRAM ACCOUNTABILITY

Trochu designates a position and individual who is accountable for implementing and maintaining access to information and privacy for information under the custody or control of Trochu.

B. OPENNESS

Trochu develops and follows access, privacy and security policies and practices that are compliant with legislation. Such policies and practices are publicly available.

C. COLLECTION OF PERSONAL INFORMATION

Trochu collects personal information only for authorized purposes and collects the least amount of personal information with the highest degree of anonymity required for the authorized purpose.

D. IDENTIFYING PURPOSES

When collecting personal information directly from an individual, the individual is informed of the purpose for which the information is collected.

E. LIMITED USE, AND DISCLOSURE OF PERSONAL INFORMATION

Personal information is only used and disclosed in accordance with the purpose for which it was collected, unless alternate use or disclosure is authorized or required by law, or with the knowledge and consent of the subject individual.

F. ACCURACY

Trochu makes all reasonable efforts to ensure that both general information and personal information created or received by Trochu is accurate and complete. Individuals who believe there is an error or omission in their personal information have a right to request correction or amendment of the information.

G. RIGHT OF ACCESS

Individuals have a right of access to all information, including personal information about themselves, that is in Trochu custody or control, subject to limited and specific exceptions.

H. SAFEGUARDS

Trochu protects personal information in its custody or control by deploying security measures and practices to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or destruction.

I. CHALLENGES

Individuals are encouraged to bring any concerns or issues regarding privacy and access at Trochu to the Privacy and Access Officer for discussion and response. The Privacy and Access Officer will investigate and respond to the individual. Individuals may appeal to the Information and Privacy Commissioner of Alberta to review or investigate Trochu right of access or correction responses, or any policies or practices that they feel are not in compliance with legislative requirements.

IV. ROLES AND RESPONSIBILITIES

A. HEAD

1. Unless otherwise delegated, the Head of Trochu is responsible for all obligations and discretionary decision-making under ATIA and POPA.
2. The Head of Trochu is recognized as Chief Administrative Officer.
3. The Head of Trochu acts as the Privacy and Access Officer.

B. PRIVACY AND ACCESS OFFICER (PAO)

The PAO is responsible for the overall management and coordination of privacy, security and access to information at Trochu. The PAO is responsible for following functions and activities:

1. PROGRAM MANAGEMENT

- a) Ensuring that privacy, access and security program policies and procedures are developed, maintained, and updated, compliant with legislation.
- b) Developing and completing quality assurance processes for implementation of Trochu organization privacy and access management.
- c) Providing training and resources so that Trochu employees, volunteers and contracted personnel are fully knowledgeable of their privacy and access duties, roles, responsibilities and practices in compliance with policy and legislation.
- d) Representing Trochu in dealings with third parties, the provincial government, and the Office of the Privacy Commissioner of Alberta, as necessary.

2. RIGHT OF ACCESS, CORRECTION, AND COMPLAINTS

- a) Responding to requests for access to information including, as necessary, assessment of fees, time extensions, disregarding requests, transfer of requests, duty to assist applicants, application of exceptions, third party notifications and public interest disclosure notice.
- b) Responding to request for correction of personal information, including, as necessary, transfer of requests, correcting personal information, annotating personal information, notifying recipients.
- c) Responding to requests for review of the handling of an access request or a privacy complaint including, as necessary, complaint submission, duty to assist the applicant, communicating with the OIPC, investigation, and responding to the applicant.

3. PRIVACY AND SECURITY

- a) In consultation with Trochu employees, providing advice, interpretation and implementation of applicable legislation regarding personal information, including release / non-release, collection, use and disclosure of personal information.

- b) Maintaining the security, protection and accuracy of personal information in the custody or control of Trochu in compliance with legislation and policy.
- c) Directing the response to privacy breaches of personal information at Trochu and its facilities in line with legislation and the Privacy Breach Response Policy.
- d) Completing Privacy Impact Assessments (PIAs) for Trochu for project-specific personal information systems and practices.
- e) Developing and maintaining a directory of Personal Information Banks and working towards developing a Personal Information Inventory as required for identifying and tracking the collection, use, disclosure and security of personal information.

C. COUNCIL AND SENIOR MANAGEMENT

- 1. Mayor and Council and Senior Management are responsible for ensuring that the Privacy Management Program, privacy, access and security policy and practices in Trochu are aligned with governing mandates, standards, and planning.

D. INFORMATION TECHNOLOGY MANAGEMENT

- 1. IT Management in coordination with the PAO, for all systems, networks, applications:
 - a) implements and deploys privacy and security measures;
 - b) completes risk and mitigation assessments;
 - c) monitors and detects security threats;
 - d) assists in the response to privacy breaches.

E. ALL TROCHU EMPLOYEES AND SERVICE PROVIDERS

- 1. All Trochu employees and service providers are responsible for implementing privacy and security for all information they create and receive as part of their functions and activities. Employees:
 - a) make themselves aware of and adhere to privacy, access and security and standards;
 - b) at the time of hire or engagement complete oath of confidentiality (Appendix 1);
 - c) capture, manage, access, release and protect information in their custody or control according to the Privacy Management Program, privacy, access and security policy;
 - d) refer to the PAO all decisions about collection, use, disclosure, and access that are not clearly directed by policy;
 - e) report all suspected breaches to personal information to the PAO immediately upon discovery;
 - f) identify and report information security incidents to the appropriate management according to privacy breach procedures.

V. QUALITY CONTROLS AND ASSURANCE

A. POLICY REVIEW

1. Trochu reviews and assesses the Privacy Management Program policies annually to ensure that they are effective and align with legislative, regulatory or Trochu functional developments and changes.

B. TRAINING AND COMMUNICATION

1. All Trochu employees are provided with regular training resources to ensure they adequately understand and can implement all aspects of the Privacy Management Program. Training is ongoing and refreshed or expanded upon in regular intervals, at onboarding and at a minimum every four years thereafter, in accordance with the roles and responsibilities of employees.
2. Training resources are reviewed annually to ensure that they are effective and align with legislative, regulatory or Trochu functional developments and changes.

C. PRIVACY, ACCESS, AND SECURITY MONITORING AND ASSESSMENT

1. Systems, circumstances, practices or repositories that pose a potential risk or gap in standards relating to the privacy, accessibility, usability, integrity, retention, continuity, and security of Trochu information are identified, monitored and assessed to determine the extent of the risk and the mitigation required.
2. Trochu has established requirements for audit logging, monitoring and review of electronic systems that collect, use, disclose or store personal information, data derived from personal information and non-personal data.

D. PERSONAL INFORMATION INVENTORY AND PERSONAL INFORMATION BANKS

1. Trochu is committed to the responsible management, protection and transparency of personal information in its custody or under its control. In support of this commitment Trochu supports the development and maintenance of a personal information inventory.
2. A personal information inventory is a comprehensive list of all personal information held by Trochu. It includes data storage locations, categories of personal information categories of individual whose personal information it holds, the purposes for collection, use and disclosure and the sensitivity and security classification of this personal information. The personal information inventory may be incorporated in records management systems and processes.
3. Trochu creates and maintains a directory of the personal information banks under its custody and control.
4. Trochu publishes the directory of its personal information banks, either in printed or electronic form, and makes it available to the public.

5. The personal information bank directory includes:
 - a) the title of the personal information bank;
 - b) the location of the personal information bank;
 - c) a description of the types of personal information included;
 - d) a description of the categories of individuals whose personal information is included;
 - e) the authority for collecting the personal information;
 - f) the purposes for which the personal information was collected or compiled; and,
 - g) the purposes for which the personal information may be used or disclosed.
6. If personal information is used or disclosed for a purpose other than the one described in the directory, Trochu
 - a) keeps a record of the purpose and connects that record to the personal information; and
 - b) updates the directory to include the new purpose in the next publication of the directory.

E. PRIVACY IMPACT ASSESSMENTS

1. Privacy Impact Assessments (PIAs) are completed for any systems, programs, services, projects or practices that introduce significant new or expanded collection, use, disclosure, processing or security exposure of personal information.
2. The introduction of, or change to, a system, program, service, project or practice is considered significant if:
 - a) the loss of, unauthorized access to or unauthorized disclosure of the personal information involved could result in significant harm;
 - g) it involves highly sensitive information;
 - h) it involves personal information of a significant percentage of the Trochu's service population;
 - i) there is data matching of personal information with an external electronic information repository;
 - j) it is part of a common or integrated service or program;
 - k) the technology used is innovative; or
 - l) the administrative, technical, or physical measures and systems being proposed represent an additional risk to the privacy of individuals.
3. Any projects or changes of such nature are reported to the Privacy and Access Officer, who is responsible for completing the PIA.

4. PIA content standards follow requirements set by the Office of the Privacy Commissioner of Alberta. The PIA is completed and submitted to the Office of the Privacy Commissioner of Alberta.

VI. TERMS AND DEFINITIONS

A. AI INFERENCE

The process by which a trained AI model takes input data and produces an output, based on conclusions and reasoning.

B. ARTIFICIAL INTELLIGENCE SERVICE (AI SERVICE)

Computer programs and applications that complete tasks and generate information that normally requires human intelligence such as evaluation, problem-solving, reasoning, and decision-making, using machine-based learning. Also considered an automated system.

C. AUTHORIZED REPRESENTATIVE

Any person who can exercise the rights or powers of an individual. This includes the right of access to an individual's personal information and the power to provide consent for disclosure of such information. This may include:

1. An executor or administrator of the estate of an individual who is deceased, for purposes of administering the estate
2. A guardian or trustee of a dependent adult, according to appointment under law
3. An agent under a personal directive, in accordance with the directive
4. An individual who is acting under specific provisions of a power of attorney
5. A guardian of a minor under 18 years of age, excluding mature minors, if the exercise of the rights or powers of the guardian would not be an unreasonable invasion of the personal privacy of the minor
6. An individual acting with the written authorization of an individual

D. COLLECTION

To gather, acquire or obtain personal information about an individual, from any source, including third parties.

E. COMMON OR INTEGRATED SERVICE OR PROGRAM

A program or service planned, administered, delivered, managed, monitored or evaluated by Trochu working collaboratively with one or more other public bodies or another public body working on behalf of Trochu or Trochu and one or more other public bodies.

F. CONFIDENTIALITY

A condition or status in which collection, use, or disclosure of information is restricted to specific persons for specific purposes. When and how the collection, use and disclosure restrictions are applied and maintained are defined by legislation and policy.

G. CONSENT

Informed agreement by an individual to the use or disclosure of their own personal information held by a public body, which can be revoked by the individual at any time.

H. CUSTODY OR CONTROL

Custody is the effective physical possession of information; control is responsibility and accountability for making decisions about the handling of information, regardless of whether Trochu has custody of the information. Trochu has control over any information that any of its officials, employees, or service providers has created or received as part of their mandated functions and activities, regardless of the location of the information or the time of collection, use, or disclosure.

I. DATA DERIVED FROM PERSONAL INFORMATION

Data created or derived from data matching that identifies individuals whose personal information was used in the data matching process. May include AI Inferences.

J. DATA MATCHING

Linking of personal information between 2 or more databases or other electronic sources of information.

K. DISCLOSURE

Giving access to or making the personal information in Trochu's custody or control available to a person or organization external to Trochu.

L. EMPLOYEE

All employees, including board members, directors, officers, contractors, students, and volunteers providing services on behalf of Trochu.

M. EXTERNAL NETWORKED SOURCE

Interconnected computer networks, such as the internet, that contain information for which Trochu has little to no control over content creation, integrity or disclosure.

N. HIGH SENSITIVITY INFORMATION

Personal information about an individual that is:

1. Biometric information
2. Financial information
3. Personal information about a minor, senior or vulnerable person

O. INDIVIDUAL

Any person, living or deceased, regardless of residency, citizenship, or status. In addition, the authorized representative of the individual.

P. LARGE LANGUAGE MODEL (LLM)

The language model of an AI Service that has been trained using vast amounts of data to learn patterns and language that generate human-like inferences.

Q. LAW ENFORCEMENT

Policing, including criminal intelligence operations, security or administrative investigation that leads or could lead to a penalty or sanction.

R. MATURE MINOR

An individual under the age of 18 who has the capacity to make their own decisions about significant matters affecting them, demonstrated by their independence, psychological stability, intellectual capacity, and/or life situation. In the case of privacy, the guardian of a mature minor would not be considered their authorized representative.

S. NOTIFICATION

An explanation of policies, procedures, consequences, and risks related to the collection, use or disclosure of an individual's personal or personal employee information. Trochu must properly inform and notify individuals and employees that personal information is being collected, the purposes for which it is being collected, and who may be contacted at Trochu if an individual has questions about the management of their personal information.

T. NON-PERSONAL DATA

Data, including data derived from personal information and synthetic data, that has been generated modified or anonymized so that it does not identify any individual.

U. PERSONAL EMPLOYEE INFORMATION

Personal information collected, used, or disclosed solely for the purposes of establishing, managing, or terminating an employment or volunteer relationship.

V. PERSONAL INFORMATION

Information about an identifiable individual including:

1. Name
2. Address, telephone, email, or contact information*

*Home or business address, telephone, email or other contact information of an employee of a public body, or any individual is not personal information, if it is provided on behalf of the employer in the individual's capacity as employee or agent.

3. Race
4. National or ethnic origin
5. Colour
6. Religion
7. Political beliefs or associations
8. Age
9. Sex
10. Gender
11. Marital status

12. Family status
13. Identifying numbers
14. Fingerprints or blood type
15. Educational, financial, employment, criminal records
16. Opinions about the individual
17. Individual's personal views or opinions (except opinions about others)

Personal information under ATIA/POPA not normally excepted from disclosure:

1. Opinions contained in work product
2. Classification, salary range, discretionary benefits, or employment responsibilities of public body employees
3. Financial and other details of a contract to supply goods or services to a public body
4. Information about a license, permit, financial or other discretionary benefit granted to an individual by a public body
5. Information is about an individual who has been dead for 25 years or more
6. Information is about an individual's enrolment at a school, attendance at a public event, or receipt of an award granted by a public body

W. PERSONAL INFORMATION BANK (PIB)

An information repository that is organized or retrievable by an individual's name or other identifier.

X. PRIVACY IMPACT ASSESSMENT (PIA)

A review and explanation of proposed changes in practices, programs or information systems affecting the collection, use, disclosure, or security of personal information under the custody or control of a public body. At the early stages, the PIA will identify practices and risks that should be addressed, amended or mitigated before implementation of the program or system.

Y. PROMPT

A cue, instruction, or question given to an AI Service to elicit a response, action, or creative output.

Z. REASONABLE SECURITY ARRANGEMENTS

Administrative, physical and technical safeguards to protect personal information, data derived from personal information and non-personal data in the custody or under the control of Trochu that are appropriate and proportional with the security classification level of the information and in the case of non-personal data, ensure to the extent possible, that the identity of the an individual who is the subject of non-personal data cannot be re-identified from the data.

AA. RECORD

Information in any form, including any electronic record or other record in any form in which information is contained or stored, including information in any written, graphic, electronic, digital, photographic, audio or other medium, but does not include any software or other mechanism used to store or produce the record.

BB. RESEARCH

Academic, applied, or scientific research, excluding internal program or quality improvement assessments, that necessitates the use of individually identifying personal information.

CC. SEVERING

In a right of access request, separating or hiding/redacting information in a document that should or cannot be released so that the remainder of the document can be disclosed.

DD. SIGNIFICANT HARM

Harm that results from the unauthorized access, disclosure, or loss of personal information, including:

1. Bodily harm
2. Humiliation
3. Damage to reputation or relationships
4. Loss of employment or business or professional opportunities
5. Identify theft
6. Diminished insurability
7. Diminished credit
8. Loss of property or legal status
9. Loss of finances

The following factors are also considered in determining the significance of harm:

1. It is reasonably believed that the information has been or will be misused
2. The unauthorized access, disclosure or loss was the result of malicious intent
3. The personal information is sensitive
4. Existing mitigating factors reduce the risk of significant harm

EE. THIRD PARTY

A person, a group of persons or an organization other than the applicant making an access request, or other than the employees and officials of Trochu.

FF. USE

Use of information by Trochu employees for an authorized purpose that is authorized by policy or law.