Policy owner:	Administration	**Policy:**	ADM 2
Adoption date:	May 19, 2026	**Effective date:**	May 19, 2026
Resolution:	2026/218	**Last amended:**	October 20, 2026

PURPOSE

Cypress County is committed to protecting the privacy of individuals whose personal information is collected, used, stored, and disclosed while delivering municipal services.

This Privacy Management Program (PMP) establishes Cypress County's framework for managing personal information in accordance with section 25 of Alberta's Protection of Privacy Act (POPA) and the Protection of Privacy (Ministerial) Regulation (M-Reg 143/2025).

The purpose of this PMP is to:

- Define the Cypress County's obligations regarding personal information
- Establish consistent privacy practices across all departments
- Set out roles and responsibilities for privacy management
- Provide procedures for handling personal information throughout its lifecycle
- Support compliance, accountability, and transparency under applicable legislation

This PMP is a living document and will be reviewed and updated as legislation, technology, and Cypress County operations evolve.

SCOPE

This PMP applies to:

- All Cypress County employees
- Elected officials
- Volunteers acting on behalf of Cypress County
- Contractors, consultants, and service providers handling Cypress County information
- All departments, programs, and services
- All personal information under the custody or control of Cypress County, regardless of format (paper or electronic)

This PMP applies throughout the full lifecycle of personal information, including collection, use, disclosure, storage, retention, and disposal.

ABOUT CYPRESS COUNTY

Cypress County is a municipal government providing services to residents, businesses, and stakeholders within its jurisdiction. In delivering these services, Cypress County collects and manages personal information necessary for program and service delivery.

LEGISLATIVE FRAMEWORK

Cypress County operates under the following legislative framework:

- **Protection of Privacy Act (POPA)** – Governs collection, use, and disclosure of personal information
- **Access to Information Act (ATIA)** – Governs access to records held by public bodies
- **Protection of Privacy Regulation** – Establishes requirements for Privacy Management Programs
- **Municipal Government Act (MGA)** – Governs municipal administration and accountability
- **Health Information Act (HIA)** – Applies where health-related information is collected or managed

Where there is a conflict between legislation and internal policy, legislation prevails.

RECORDS MANAGEMENT AND ATIA COORDINATOR DESIGNATION

1. Designated Records Management and ATIA Coordinator

Cypress County designates a Records Management and ATIA Coordinator responsible for overseeing privacy compliance and implementation of this PMP.

2. Responsibilities of the Records Management and ATIA Coordinator

The Records Management and ATIA Coordinator is responsible for:

- Leading implementation and maintenance of this PMP
- Ensuring compliance with POPA and ATIA
- Acting as the primary contact for privacy matters
- Coordinating responses to privacy incidents and breaches
- Reviewing Privacy Impact Assessments (PIAs)
- Liaising with the Office of the Information and Privacy Commissioner (OIPC)
- Delivering or coordinating privacy training
- Monitoring legislative and regulatory changes
- Maintaining privacy documentation and supporting tools

3. Privacy Accountability Structure

Privacy responsibilities are shared across the organization:

Role	Responsibility
Council	Provides governance oversight and ensures accountability
Chief Administrative Officer (CAO)	Operational accountability and resourcing
Records Management & ATIA Coordinator	Leads privacy program implementation
Department Managers	Ensure compliance within their areas
Employees	Follow privacy requirements and report incidents
IT Services	Implement technical safeguards and system protections

COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION

1. Definition of Personal Information

Personal information means recorded information about an identifiable individual, including:

- Name and contact information
- Identification numbers
- Financial or employment information
- Opinions or views about an individual
- Any information that can identify an individual directly or indirectly

2. Collection of Personal Information

Cypress County collects personal information only where authorized under POPA or other applicable legislation, including:

- Where required or permitted by law
- Where necessary for municipal operations or service delivery
- With informed consent, where applicable

3. Notice of Collection

When collecting personal information directly, Cypress County will provide notice of:

- Legal authority for collection
- Purpose of collection
- Contact information for the Records Management and ATIA Coordinator

Only information necessary for the identified purpose will be collected.

4. Use of Personal Information

Personal information will only be used for:

- The purpose for which it was collected
- A consistent or related purpose
- A purpose authorized by legislation
- A purpose for which consent has been provided

Access is restricted to authorized staff on a **need-to-know basis**.

5. Disclosure of Personal Information

Personal information will only be disclosed where:

- Authorized or required by legislation
- Consent has been provided
- Required by legal process (court order, subpoena, warrant)
- Permitted for law enforcement purposes

Only the minimum necessary information will be disclosed.

6. Consent

Where consent is used, it must be:

- Informed

- Voluntary
- Specific
- Documented

Consent is not required where legislation authorizes collection, use, or disclosure. Individuals may withdraw consent where applicable, subject to legal or operational limits.

Correction of Personal Information

1. Right to Request Correction

Individuals may request correction of personal information held by Cypress County under POPA.

2. Correction Process

- Individual submits a written request to the Records Management and ATIA Coordinator
- Records Management and ATIA Coordinator acknowledges receipt within 10 business days
- Cypress County reviews accuracy and completeness of the information
- If corrected, updates are made and third parties are notified where appropriate
- If not corrected, the record is annotated and reasons are provided in writing

3. Response Time

Cypress County will respond to correction requests within **45 business days**, unless otherwise required by legislation.

Privacy Incidents and Breach Notification

1. Definition of a Privacy Incident

A privacy incident includes any unauthorized access, collection, use, disclosure, loss, or destruction of personal information under Cypress County's custody or control.

2. Incident Response Process

Step 1 – Identify and Contain

Employees must immediately take steps to contain the incident and report it to their supervisor and the Records Management and ATIA Coordinator without delay.

Step 2 – Assess

The Records Management and ATIA Coordinator assesses:

- Nature of the incident
- Type of information involved
- Individuals affected
- Risk of harm

Step 3 – Notification

Where a real risk of significant harm exists, Cypress County will notify:

- The Office of the Information and Privacy Commissioner (OIPC)
- Affected individuals

Step 4 – Remediation

Corrective actions are implemented to prevent recurrence.

Step 5 – Documentation

All incidents are recorded in a Privacy Incident Log maintained by the Records Management and ATIA Coordinator.

3. Privacy Incident Log

Cypress County maintains a log of all privacy incidents including:

- Date of incident
- Description
- Information involved
- Number of individuals affected
- Risk assessment outcome
- Notifications made
- Corrective actions taken

4. Supporting Guidance

Cypress County will use OIPC guidance tools to support consistent assessment and reporting of privacy incidents.

Privacy Impact Assessments (PIAs)

1. Purpose

Cypress County is required under the **Protection of Privacy Act (POPA)** to assess privacy risks before implementing new or significantly modified programs, systems, or processes involving personal information.

A Privacy Impact Assessment (PIA) is a structured review used to identify, evaluate, and mitigate privacy risks prior to implementation.

2. When a PIA is Required

A PIA must be completed prior to:

- Introducing any new program, service, or initiative involving personal information
- Making significant changes to existing programs that affect how personal information is collected, used, or disclosed
- Implementing new technology systems that process personal information
- Engaging third-party service providers who will access personal information
- Implementing data-sharing, integration, or automated decision-making systems (including AI tools where applicable)

The Records Management and ATIA Coordinator is responsible for determining whether a formal submission to the Office of the Information and Privacy Commissioner (OIPC) is required.

3. PIA Process

3.1. Department identifies a new or changed initiative involving personal information

3.2. Department notifies the Records Management and ATIA Coordinator at the earliest planning stage

3.3. A preliminary privacy risk assessment is completed

3.4. Records Management and ATIA Coordinator determines whether a full PIA is required

3.5. Department prepares the PIA using the OIPC-approved template, with support from the Records Management and ATIA Coordinator

3.6. Records Management and ATIA Coordinator reviews, validates, and approves the PIA

3.7. If required, the PIA is submitted to the OIPC prior to implementation

3.8. Approved PIAs are retained as part of Cypress County's privacy compliance records and reviewed if material changes occur

4. Key Principle

No program, system, or service involving personal information should proceed to implementation until privacy risks have been appropriately assessed and approved.

5. Resources

- OIPC PIA Template (ATIA/POPA resources)
- OIPC PIA Guidance Materials
- OIPC Privacy Risk Assessment Tools

Protection and Security of Personal Information

1. Overview

Cypress County will implement reasonable administrative, physical, and technical safeguards to protect personal information against unauthorized access, collection, use, disclosure, loss, or destruction.

Security measures are designed to be proportional to the sensitivity of the information and the risks associated with its use.

2. Administrative Safeguards

- Privacy policies and procedures under this PMP
- Mandatory privacy training for all staff
- Role-based access to personal information
- Confidentiality requirements for employees and contractors
- Defined retention and disposal practices
- Periodic internal privacy reviews

3. Physical Safeguards

- Secure storage for paper records containing personal information
- Controlled access to facilities and records storage areas
- Clean desk expectations in areas handling personal information
- Secure disposal of physical records (approved shredding or destruction methods)
- Visitor access controls where appropriate

4. Technical Safeguards

- Password-protected systems and secure authentication methods
- Role-based system access controls
- Encryption of sensitive data where appropriate
- Secure network infrastructure and monitoring tools

- Logging and audit trails for system access
- Regular patching and system updates
- Secure backup and recovery procedures

5. Information Lifecycle Management

Personal information is managed throughout its lifecycle:

- **Collection:** Limited to what is necessary for the identified purpose
- **Use:** Restricted to authorized and consistent purposes
- **Storage:** Protected through appropriate safeguards
- **Retention:** Retained only as long as required by law or operational need
- **Disposal:** Securely destroyed or de-identified when no longer required

Contracting with Service Providers

1. Accountability

Cypress County remains accountable for personal information in its custody or control, even when it is handled by third-party service providers.

2. Due Diligence

Before engaging a service provider that will handle personal information, Cypress County will:

- Assess the provider's privacy and security practices
- Determine whether a PIA is required
- Confirm the provider can meet POPA obligations
- Evaluate data handling and storage locations where applicable

3. Contract Requirements

All contracts involving personal information must include provisions requiring service providers to:

- Use personal information only for authorized purposes
- Protect personal information using safeguards equivalent to Cypress County standards
- Report privacy incidents without delay
- Return or securely destroy personal information at contract end
- Permit reasonable audit or verification of compliance
- Obtain approval before subcontracting data handling responsibilities

4. Oversight

The Records Management and ATIA Coordinator maintains a register of active service provider agreements involving personal information and may conduct periodic compliance reviews.

Privacy Training and Awareness

1. Purpose

A strong privacy culture is essential to protecting personal information and meeting legislative obligations under POPA and ATIA.

2. Mandatory Training

All employees, elected officials, volunteers, and applicable contractors must complete privacy

training appropriate to their role.

Training includes:

- Overview of privacy legislation (POPA and ATIA)
- Responsibilities for handling personal information
- Recognizing and reporting privacy incidents
- Proper collection , use, storage, and disposal practices
- Consequences of privacy non-compliance

3. Training Requirements

Training Type	Audience	Timing
General Privacy Awareness	All staff, officials, volunteers	Onboarding and annually
Legislative Foundations	All staff	Upon hire and when updated
Role-Specific Training	Staff handling sensitive data	As required or role change
Advanced Privacy Training	Records Management and ATIA Coordinator, leadership, IT	As needed or legislative change
Incident/Breach Response Training	Managers, Records Management and ATIA Coordinator, IT	Annual refresh

4. Training Records

Cypress County will maintain records of completed privacy training as part of employee documentation. Training compliance may be monitored to ensure ongoing adherence to this PMP.

Handling Privacy Complaints

1. Purpose

Cypress County provides an internal process for addressing privacy-related complaints in a timely and transparent manner before escalation to the Office of the Information and Privacy Commissioner (OIPC).

Individuals may submit concerns regarding Cypress County's collection, use, or disclosure of personal information.

2. Internal Complaint Process

2.1. The individual submits a privacy complaint to the Records Management and ATIA Coordinator (written or verbal; verbal complaints will be documented)

2.2. The Records Management and ATIA Coordinator acknowledges receipt within **5 business days**

2.3. The Records Management and ATIA Coordinator reviews and investigates the complaint, which may include:

2.3.1. Reviewing records

2.3.2. Consulting relevant staff

2.3.3. Seeking legal or policy guidance where required

2.4. A written response is provided within **30 business days**, outlining:

2.4.1. Findings

2.4.2. Any corrective actions taken

2.4.3. Outcome of the review

2.5. If the complainant is not satisfied, they may submit a complaint to the OIPC

3. External Complaint Process (OIPC)

Individuals may submit a complaint directly to the OIPC at any time.

The County will cooperate fully with any OIPC investigation, including providing records and information as required under ATIA and POPA.

Access to Information

1. Overview

The **Access to Information Act (ATIA)** provides individuals with the right to access records held by Cypress County, subject to applicable exceptions.

Cypress County designates an ATI Coordinator responsible for managing access requests.

2. ATI Coordinator

- **Position Title:** Records Management and ATIA Coordinator
- **Name:** Kathy Patton
- **Phone:** 403-526-2888 Ext. 328
- **Email:** kathy.patton@cypress.ab.ca

3. Access Request Process

Individuals may submit an access request to the ATI Coordinator.

Cypress County will:

- Acknowledge receipt promptly
- Process requests within legislated timelines under ATIA
- Apply exemptions only where authorized by law
- Provide assistance to requesters to clarify or refine requests where needed

Cypress County is committed to a duty to assist principle throughout the access process.

Automated Systems and Artificial Intelligence

1. Purpose

Cypress County recognizes that automated systems, including artificial intelligence tools, may process personal information and therefore require appropriate privacy controls under POPA.

2. Current Use

Cypress County will document whether automated decision-making or AI systems are currently in use. Where such systems are not in use, Cypress County will review and assess any future adoption prior to implementation.

3. Requirements for Automated Systems

Where automated systems are used, Cypress County will ensure:

- Personal information used by the system is documented
- The purpose and function of the system is clearly defined
- Security and technical safeguards are implemented
- Derived data produced by the system is identified and controlled
- A PIA is completed prior to implementation
- Individuals are notified where automated decisions significantly affect them
- A process exists for individuals to challenge or request review of automated decisions

4. Data Matching

All data matching activities must comply with POPA requirements.

- A PIA is required prior to initiation
- Records Management and ATIA Coordinator approval is mandatory
- Data sharing must be limited to authorized purposes only

Non-Personal Data

1. Definition

Non-personal data refers to information derived from personal information that has been de-identified so that individuals cannot reasonably be identified.

2. Policy

Cypress County will ensure that any creation, use, or disclosure of non-personal data:

- Is properly de-identified using appropriate techniques
- Cannot reasonably be re-identified
- Is used only for authorized purposes
- Is governed by appropriate agreements where shared externally

The County will not permit re-identification of de-identified datasets.

Public Transparency and Availability

1. Access to this PMP

Cypress County is committed to transparency and will make this PMP available to the public.

This PMP may be accessed through:

- Cypress County website: Cypress County - Access to Information/Privacy Policy
- A written request to Cypress County Administration Office

Requests will be fulfilled within **30 business days**, where practicable.

Review and Maintenance

2. Review Schedule

This PMP is reviewed:

- Annually
- When legislation changes
- Following a significant privacy incident

- When new programs or technologies are introduced
- When organizational structure changes affect privacy responsibilities

Appendices

1. Appendix A – PMP Compliance Checklist

Cypress County will maintain compliance with POPA regulatory requirements as follows:

Core Requirements

- Records Management and ATIA Coordinator designated
- Correction request procedures established
- Privacy incident response procedures documented
- Complaint handling process defined
- Security safeguards implemented (administrative, physical, technical)
- Service provider requirements established
- Privacy training program implemented
- PIA process documented
- Public access to PMP ensured
- Annual review process established

Enhanced Requirements (as applicable)

- Defined accountability structure
- Formal PIA process including submission requirements
- Consent management principles
- Automated systems / AI governance
- Data matching controls
- Non-personal data governance

External Resources

- Office of the Information and Privacy Commissioner (OIPC) https://oipc.ab.ca
- ATIA/POPA Resources https://oipc.ab.ca/atia-popa-resources/
- Access to Information Act https://alberta.ca/access-to-information-act
- Protection of Privacy Act https://alberta.ca/protection-of-privacy-act

History

Amendment Dates & Description	Resolution No. 2026/423 – October 20, 2026
Review Dates & Outcomes	