



COUNTY OF NEWELL

PRIVACY MANAGEMENT PROGRAM

Established pursuant to the *Protection of Privacy Act* (POPA)
and the Protection of Privacy (Ministerial) Regulation (M-Reg 143/2025)

Effective date:	June 11, 2026
Version	1.0
Approved by:	Records & Information Governance Committee
Next Review:	June 30, 2027
Classification:	Public

QUICK REFERENCE

This document describes the County of Newell's Privacy Management Program, including:

- What we do to protect personal information
- Who is responsible
- What you can do if you have questions or want to access or correct your information
- How to make a privacy complaint

This Privacy Management Program is established under section 25 of Alberta's *Protection of Privacy Act*.

I want to...	What I do
Understand how the County of Newell handles privacy	Read this guide
See what kinds of personal information the County holds	See "Personal Information Banks" or visit countyofnewell.ab.ca/privacy-policy
See or correct my own personal information	See "Your Rights"
Know who to contact about privacy	See "Designation of Privacy Officer"

This document does not include specific technical information, security-related information, or other details that could make our systems vulnerable to attack and compromise the security of personal information under our custody and control. (M-Reg 143/2025 s. 6(4))

TABLE OF CONTENTS

1.	Introduction	4
A.	Purpose	4
B.	Scope	4
C.	About the County of Newell	4
D.	Legislative Framework	4
2.	Designation of Privacy Officer & ATI Coordinator	5
A.	Designated Privacy Officer & ATI Coordinator	5
B.	Privacy Accountability Structure	5
3.	Collection, Use, & Disclosure of Personal Information	6
A.	Definition of Personal Information	6
B.	Collection of Personal Information	6
C.	Use of Personal Information	6
D.	Disclosure of Personal Information	7
E.	Consent	7
F.	Personal Information Banks (PIBs)	7
4.	Your Rights	8
A.	Access	8
B.	Correction of Personal Information	8
C.	Requesting a Review by the OIPC	8
5.	Privacy Incidents & Breach Notification	10
A.	What is a privacy breach?	10
B.	Incident Response Procedure	10
6.	Privacy Impact Assessments (PIAs)	11
7.	Protection & Security Arrangements	12
A.	Administrative safeguards	12
B.	Physical safeguards	12
C.	Technical safeguards	12
D.	Information lifecycle	12
E.	Security Classification	13
8.	Contracted Service Providers	14
9.	Privacy Training & Awareness	15
10.	Privacy Complaints	8
11.	Automated Systems and Artificial Intelligence	16
A.	Current Status	16
B.	Policy Requirements for Automated Systems & AI	16
C.	Data Matching	16
12.	Non-Personal Data	17
13.	Personal Information Banks (PIBs)	18
14.	Review & Maintenance	19
15.	Legal Obligations	21

1. INTRODUCTION

A. PURPOSE

The County of Newell (the County) recognizes the importance of protecting the privacy rights of all Albertans and all employees are committed to protecting any personal information that we collect, use and disclose. This Privacy Management Program (PMP) fulfills the County's legal obligation under section 25 of Alberta's Protection of Privacy Act (POPA) and the Protection of Privacy (Ministerial) Regulation (M-Reg 143/2025).

The PMP sets out the documented policies, procedures, roles, and tools that govern how the County manages personal information. This document is reviewed regularly and updated to reflect changes to the County's programs, implementation of new technology, and changes to legislative requirements.

Under POPA, any person may request a copy of the County's PMP. The County is committed to transparency and makes this PMP available upon the County's website: <https://countyofnewell.ab.ca/access-and-privacy>

Paper copies are available upon request at the County office.

B. SCOPE

The PMP applies to:

- All County employees, elected officials, and volunteers
- All contractors, consultants, and service providers acting on behalf of the County
- All County departments, programs, and services that collect, use, store, or disclose personal information
- All personal information held in any format – paper or electronic

C. ABOUT THE COUNTY OF NEWELL

The County of Newell is a municipal district in southeastern Alberta. As a public body under POPA, the County provides a wide range of services to residents, ratepayers, and stakeholders including (but not limited to) land use planning, development, roads, infrastructure, agricultural services, emergency management, and utilities. These services require the collection of personal information from members of the public.

D. LEGISLATIVE FRAMEWORK

Key legislation:

- [Protection of Privacy Act \(POPA\)](#)
In force June 11, 2025; replaces FOIP privacy provisions
- [Protection of Privacy \(Ministerial\) Regulation](#) (M-Reg 143/2025)
Outlines PMP requirements
- [Protection of Privacy Regulation](#) (Reg 132/2025)
Definitions for interpretation of POPA (consent, reasonable security arrangements)
- [Access to Information Act \(ATIA\)](#)
In force June 11, 2025; governs access to information requests
- [Municipal Government Act \(MGA\)](#)
Governs the County's operations and accountability

2. DESIGNATION OF PRIVACY OFFICER & ATI COORDINATOR

A. DESIGNATED PRIVACY OFFICER & ATI COORDINATOR

Section 6(1)(a) of M-Reg 143/2025 requires every public body to designate a Privacy Officer responsible for ensuring the County's compliance with POPA.

The County's ATIA & POPA Bylaw designates the position responsible for ensuring the County's compliance with POPA and ATIA.

Position Title:	Executive Assistant
Name:	Ariana Nielsen
Phone:	403-794-2319
E-mail:	nielsena@newellmail.ca

The Privacy Officer & ATI Coordinator is the County's primary point of accountability for privacy. Key responsibilities include:

- Overseeing the development, implementation, and maintenance of this PMP
- Ensuring all County departments comply with POPA and this PMP
- Serving as the primary contact for privacy-related inquiries from the public and staff
- Coordinating the County's response to privacy breaches and incidents
- Reviewing and approving Privacy Impact Assessments (PIAs) before submission to the OIPC
- Liaising with the Office of the Information and Privacy Commissioner (OIPC) of Alberta
- Delivering or coordinating privacy training for staff
- Monitoring legislative changes and updating this PMP accordingly
- Making this PMP available to the public upon request within 30 business days

B. PRIVACY ACCOUNTABILITY STRUCTURE

While the Privacy Officer holds primary accountability, responsibility for privacy is shared across the entire organization.

CAO	The head of the public body under POPA who holds ultimate responsibility for the County's compliance with POPA and ATIA. The CAO may, and does, delegate operational privacy to responsibilities to the Privacy Officer and ATI Coordinator, approves the PMP, and ensures there are adequate resources for privacy compliance
Privacy Officer/ ATI Coordinator	Day-to-day responsibility for access and privacy, including responding to access and correction requests, privacy complaints, PMP requests, breach reporting, PIAs, OIPC liaison and maintaining the PIB directory.
System Owners	Implement privacy practices in their programs and systems, including identifying PIBs, supporting PIAs, and escalating incidents to the Privacy Officer.
IT Department	Implement technical safeguards; support PIAs for technology systems; respond to technical breaches
All Employees	Handle personal information in accordance with POPA, this PMP, and County policies; report suspected incidents immediately

3. COLLECTION, USE, & DISCLOSURE OF PERSONAL INFORMATION

A. DEFINITION OF PERSONAL INFORMATION

Personal information means recorded information about an identifiable individual, including their name, address, contact information, financial information, employment records, and any other information that can be used to identify a person. It also includes:

- identifying numbers or symbols assigned to the individual (e.g. customer or Employee ID)
- biometric information (e.g. the individual's fingerprints or blood type)
- information about the individual's health and health care history, including information about the individual's physical or mental health (e.g. pre-employment screening results)
- anyone else's opinions about the individual (e.g. Annual Review & Performance Plan)
- the individual's personal views or opinions except if they are about another individual

B. COLLECTION OF PERSONAL INFORMATION

The County collects personal information only when:

- Expressly authorized by an enactment of Alberta or Canada,
- The information is collected for the purposes of law enforcement, or
- The information relates directly to and is necessary for an operating program or activity of the public body, including a common or integrated program or service.

Personal information will be collected directly from the individual the information is about unless another method of collection is authorized by that individual or permitted under POPA.

When collecting personal information directly from an individual, the County will provide notice of:

- The legal authority for the collection
- The purpose(s) for which the information is being collected
- The contact information for the Privacy Officer
- The County's intention, if any, at that time to enter the collected information into an automated system to generate content or make decisions, recommendations, or predictions

C. USE OF PERSONAL INFORMATION

Personal information collected by the County is used only for:

- the purpose for which the information was collected or compiled or for a use consistent with that purpose,
- a purpose for which the individual has consented
- a purpose that is permitted or required by POPA or any other enactment

Access to personal information is limited to employees who need it to perform their duties. Department managers are responsible for enforcing access controls within their programs.

D. DISCLOSURE OF PERSONAL INFORMATION

The county will not disclose personal information except:

- As required or authorized by POPA or another enactment
- With the written consent of the individual
- For law enforcement or legal proceedings purposes as permitted
- To comply with a subpoena, warrant, or court order

The County will never sell your personal information.

E. CONSENT

Where the County relies on consent as the main authority for collection, use, or disclosure of personal information, the consent must be informed and meaningful. The County will:

- Clearly explain what information is being collected and why
- Use plain language in any consent forms or notices
- Not make consent a condition of service where not necessary
- Allow individuals to withdraw consent where applicable

F. PERSONAL INFORMATION BANKS (PIBs)

A Personal Information Bank (PIB) is a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual. POPA Section 57 requires the County to maintain a directory of its PIBs that includes:

- the title and location of the personal information bank
- a description of the kind of personal information that is included
- the authority for collecting the personal information
- the purposes for which the personal information was collected, compiled, used and/or disclosed

The PIB directory is available on the County's website:

<https://countyofnewell.ab.ca/access-and-privacy>

4. YOUR RIGHTS

Below is a description of your rights about your personal information.

A. ACCESS

Under section 6 of ATIA, individuals have the right to access records held by the County, including records containing personal individual. Access requests may be submitted to the County's ATI Coordinator using the following process:

1. Submit a written request to the ATI Coordinator using the Access to Information Request form <https://www.alberta.ca/system/files/atia-access-to-information-form.pdf>
2. The ATI Coordinator will promptly acknowledge the request.
3. Processing begins once the initial fee is received.
 - a. If the request is for the applicant's own personal information, there is no initial fee.
 - b. If the request is for general information (i.e. information other than the applicant's own personal information), the initial fee is \$25.00
4. A response will be provided within thirty (30) business days unless extended under ATIA.
5. If the applicant is not satisfied with the response, they may request a review by the OIPC.

B. CORRECTION OF PERSONAL INFORMATION

Under section 7 of POPA, individuals have the right to request the correction of their personal information held by the County using the following process:

1. Submit a written correction request to the Privacy Officer using the Request to Correct Personal Information form.
<https://www.alberta.ca/system/files/popa-correction-of-personal-information-form.pdf>
Make sure to identify the specific information to be corrected.
2. The Privacy Officer must respond within thirty (30) business days, giving notice that either the correction has been made or an annotation has been created linking the record to the correction request.
3. If the information is determined to be incorrect or incomplete, the County will correct the information and send the corrected information to any party to whom the incorrect information was disclosed.
4. If the County decides not to make the requested correction, a note will be added to the record to indicate that a correction request had been received. The individual requesting the correction will be notified, in writing, of the reasons why the correction was not completed.
5. If the applicant is not satisfied with the County's decision, they may request a review by the OIPC.

C. PRIVACY COMPLAINTS

POPA Section 37 gives individuals the right to make a complaint to the OIPC about the County's collection, use, or disclosure of their personal information. Before making a request for a review by the OIPC, the individual must first submit their complaint to the County using the following process:

1. Individual submits a privacy complaint in writing to the Privacy Officer (or verbally, which the Privacy Officer will document).
2. The Privacy Officer investigates the complaint, which may involve reviewing records, interviewing staff, or consulting with legal counsel.
3. The Privacy Officer provides a written response to the complainant within thirty (30) business days after receiving the complaint, including the outcome of the investigation and any corrective action(s) taken.

4. If the complainant is not satisfied with the County's response, they may submit a written request for review to the OIPC of Alberta

D. REQUESTING A REVIEW BY THE OIPC

You may request a review by the OIPC using the appropriate forms available on their website.

Information Access Review: <https://oipc.ab.ca/information-access-review/>

OIPC Privacy/Correction Request Form: oipc.ab.ca/ati-popa-resources/

OIPC Phone: 780.422.6860 Toll-free: 1.888.878.4044

5. PRIVACY INCIDENTS & BREACH NOTIFICATION

A. WHAT IS A PRIVACY BREACH?

A privacy breach occurs when personal information under the County's custody or control is lost, accessed, used, collected or disclosed without authorization. POPA Section 10(2) requires the County to notify the OIPC and affected individuals when a privacy breach occurs that creates a real risk of significant harm (RROSH).

B. INCIDENT RESPONSE PROCEDURE

1. Identify & Contain

- When a potential breach is identified, immediate action is taken to prevent further unauthorized access or disclosure.
- The breach is immediately reported to the Departmental Supervisor and the Privacy Officer. The IT Department will also be notified if the breach involves unauthorized access to the County network.

2. Assess

- The Privacy Officer will assess the breach to determine what information was involved, who was affected, and whether RROSH exists using the OIPC Breach Assessment Tool.

3. Notify

- If RROSH exists, notification is **mandatory** to the OIPC using the POPA Breach Notification Form, the Minister responsible for POPA (Technology & Innovation) as well as the affected individuals.
- If RROSH does not exist, notification is not mandatory.

4. Remediate

- Security arrangements will be reviewed and strengthened
- Corrective actions will be taken to prevent recurrence
- All steps taken will be documented
- Privacy Impact Assessments (PIAs) will be updated if the incident reveals new risks

5. Document

- The Privacy Officer will maintain a Privacy Breach Log that includes a description of the breach, date of discovery, personal information involved, number of affected individuals, assessment outcome, notifications made, and remediation steps. The log will be reviewed annually by the Records & Information Governance Committee.

6. PRIVACY IMPACT ASSESSMENTS (PIAs)

A Privacy Impact Assessment (PIA) is used to identify and review risks associated with the County's collection, use, and disclosure of personal information and develop strategies and safeguards to mitigate those risks.

The County must complete a PIA prior to:

- Implementing any new program, project, service, or administrative practice that will collect, use, or disclose personal information
- Making substantial changes to an existing program that materially alters how personal information is handled
- Deploying new technology that processes personal information
- Entering into a new service provider agreement involving personal information
- Implementing any data matching or artificial intelligence system.

The OIPC PIA Submission Assessment Tool will be used to determine whether a PIA must be formally submitted to the OIPC. Generally, a formal submission is required when the practice, program, project, or service:

- will collect, use or disclose personal information deemed to be of high sensitivity;
- will involve the personal information of a significant percentage of the population the public body serves;
- will involve data matching between 2 or more public bodies;
- is part of a common or integrated program or service;
- involves the development or use of innovative technology;

or if the Commissioner requests a copy of a PIA.

7. PROTECTION & SECURITY ARRANGEMENTS

Under POPA, the County is required to make reasonable arrangements to protect personal information against unauthorized access, collection, use, disclosure, copying, modification, disposal, or destruction.

A. ADMINISTRATIVE SAFEGUARDS

- Privacy policies and procedures in this PMP
- Employee privacy training and awareness program (see Section 9)
- Role-based access controls — employees access only the information they need
- Confidentiality agreements and privacy clauses in employment contracts
- Formal data retention and destruction schedules
- Regular audits and reviews of access to personal information

B. PHYSICAL SAFEGUARDS

- Locked filing cabinets and secure storage for paper records containing personal information
- Controlled access to County facilities and record rooms
- Clean desk policy for workstations handling personal information
- Secure disposal of paper records
- Visitor access controls

C. TECHNICAL SAFEGUARDS

- Password-protected systems with multi-factor authentication where available
- Network security including firewalls, intrusion detection, and antivirus software
- Encrypted storage and transmission of personal information
- Regular security patches and software updates
- Access logs and audit trails for sensitive systems
- Secure backup and recovery procedures

D. INFORMATION LIFECYCLE

The County manages personal information throughout its lifecycle:

- Collection: Minimum necessary — only collect what is needed for the stated purpose
- Storage: Secure, organized, and accessible only to authorized staff
- Use: Limited to the purpose for which it was collected
- Retention: Retained only as long as necessary for the purpose, or as required by law
- Disposal: Securely destroyed when no longer required, in accordance with ARMA records schedules

E. SECURITY CLASSIFICATION

The County's Records Classification Structure lists default information security classifications for each records series. A security classification identifies the sensitivity, criticality, value, and importance of the information in a record and identifies who can have access, protecting the information from unauthorized disclosure or modification.

Classification Level	Description
Public	Applies to information, records, and data that, if compromised, will not result in harm. Accessible to all employees and generally available to the public either on the website or available upon request. Note: Classifying data or information as Public does not require that it be made available to the public (i.e. via the County of Newell website).
Internal	Applies to information, records, and data that, if compromised, may cause moderate harm to the organization and/or individuals if compromised or disclosed inappropriately. Accessible to any employee who requires it for their work
Confidential	Includes demographic personal information about staff and ratepayers. Accessed only by staff members from specified departments. May cause significant harm to the organization and/or individuals if compromised or disclosed inappropriately. Accessible only to a specific function group or role on an as-needed basis if needed for their work.
Restricted	Includes medical, disciplinary, law enforcement, financial and biometric information about employees and ratepayers, contracts, legal matters, and other highly restricted information that would cause serious harm to the organization and/or individuals if compromised or disclosed inappropriately. Accessible only to named individual(s) or specific positions on an as-needed basis for their work, subject to administrative controls.

8. CONTRACTED SERVICE PROVIDERS

The County remains responsible for any personal information required to deliver services provided by a third party through a contract.

Before engaging a service provider with access to personal information, the County will:

- Assess the service provider's privacy and security practices
- Determine whether a PIA is required for the engagement
- Confirm the service provider can meet the County's obligations under POPA

All contracts with service providers who handle personal information must include provisions requiring the service provider to:

- Collect, use, and disclose personal information only for the purposes specified in the contract
- Implement security safeguards equivalent to those required by POPA
- Notify the County immediately of any privacy breach or incident
- Return or securely destroy personal information upon contract termination
- Allow the County to audit compliance with privacy obligations
- Not sub-contract personal information handling without prior County approval

The Privacy Officer maintains a register of active service provider agreements involving personal information and conducts periodic reviews to confirm ongoing compliance.

9. PRIVACY TRAINING & AWARENESS

All employees, elected officials, and volunteers must complete privacy training that covers:

- An overview of POPA and the County's obligations
- Employee rights and responsibilities regarding personal information
- How to recognize and respond to a privacy breach or incident
- Proper handling, storage, and disposal of personal information
- Consequences of non-compliance

Training Type	Audience	Frequency
General privacy awareness	All staff, elected officials, volunteers	Upon onboarding; annually
POPA for Public Bodies (Service Alberta Online Course)	All staff, elected officials	Upon onboarding, as updated by Service Alberta
Advanced privacy training	Privacy Officer, Senior Staff, IT Department	As required; when legislation changes
Role-specific training	Staff handling sensitive information	Upon role change or as required
Breach response simulation	Privacy Officer, Senior Staff, IT Department	Annually

Staff training records are retained in the County's EDRMS and form part of the personnel files.

10. AUTOMATED SYSTEMS AND ARTIFICIAL INTELLIGENCE

Section 6(1)(b)(iii) and 6(2)(a)(v) of M-Reg. 143/2025 require public bodies to have policies governing automated systems, including artificial intelligence (AI), that use personal information.

A. CURRENT STATUS

The County does not currently use AI or automated decision-making systems that process personal information.

If the County considers implementing AI or automated decision-making systems that will process personal information, a PIA will be completed and this section will be updated.

B. POLICY REQUIREMENTS FOR AUTOMATED SYSTEMS & AI

Where the County uses automated systems or AI that processes personal information, the County must:

- Document what personal information is used by the system
- Describe any security and technical safeguards in place
- Identify any derived data created by the system about individuals
- Ensure a PIA has been conducted and submitted to the OIPC where required
- Provide meaningful notice to individuals where automated decisions are made about them
- Establish a process for individuals to question or contest automated decisions

C. DATA MATCHING

Data matching means linking personal information between two or more databases or other electronic sources of information. Any data matching activity must comply with Part 3 of POPIA. A PIA must be prepared and submitted to the OIPC before any data matching commences. The Privacy Officer must approve all data matching initiatives.

11. NON-PERSONAL DATA

Non-personal data is data derived from personal information from which all personal identifying information has been removed. POPA allows public bodies to create, use, and disclose non-personal data in limited circumstances.

Where the County creates, uses, or discloses non-personal data, it must:

- Ensure the data has been properly de-identified so that individuals cannot reasonably be identified
- Follow POPA Part 3 requirements and any applicable regulations
- Document the purposes for which non-personal data is used or disclosed
- Ensure any data sharing agreements with third parties do not permit re-identification

12. PERSONAL INFORMATION BANKS (PIBs)

A Personal Information Bank (PIB) is a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual. POPA Section 57 requires the County to maintain a directory of its PIBs that includes:

- the title and location of the personal information bank
- a description of the kind of personal information that is included
- the authority for collecting the personal information
- the purposes for which the personal information was collected, compiled, used and/or disclosed

The PIB directory is available to the public upon request OR available upon the County's website: <https://countyofnewell.ab.ca/access-and-privacy>

13. REVIEW & MAINTENANCE

The County will review the Privacy Management Program at least once every three (3) years or earlier in the event of:

- Changes to the legislation or regulation
- A significant privacy breach
- New programs or technologies are introduced
- Organizational restructuring that affects privacy responsibilities

Version Control

Version	Date	Summary of Changes	Approved by
1.0	June 2026	Initial Version	

14. LEGAL OBLIGATIONS

The tables below map each PMP requirement to the County document(s) that satisfy it.

Core Requirements – Apply to all public bodies (M-Reg 143/2025 s.6(1))

M-Reg 143/2025 Reference	Requirement	County Document(s)
s.6(1)(a)	Designation or identification of a privacy officer	Bylaw 2127-26 ATIA & POPA
s.6(1)(b)(i)(A)	Internal policies and procedures – responding to requests for correction of personal information (POPA s.7)	
s.6(1)(b)(i)(B)	Internal policies and procedures – responding to privacy incidents (POPA s10(2))	
s.6(1)(b)(i)(C)	Internal policies and procedures – responding to privacy complaints (POPA S.38(2))	
s.6(1)(b)(ii)	Internal policies and procedures – creation, use, and disclosure of non-personal data	
s.6(1)(b)(iii)	Internal policies and procedures – how automated systems will use personal information, including security and technical safeguards	
s.6(1)(c)	Security classification system for personal information, data derived from personal information, and non-personal data	
s.6(1)(d)	Mandatory training for employees, with specified retraining intervals	
s.6(1)(e)	Timelines for periodic review, assessment, and update of the PMP	

Enhanced requirements – high volume or highly sensitive personal information (M-Reg 143/2025 s.6(2))

M-Reg 143/2025 Reference	Requirement	County Document(s)
s.6(2)(a)(i)	Roles, responsibilities, and accountabilities of employees in relation to obligations under POPA	
s.6(2)(a)(ii)	Process for completing and submitting privacy impact assessments	
s.6(2)(a)(iii)	Proactive monitoring of information systems holding personal information, derived data, or non-personal data	
s.6(2)(a)(iv)	Policies and procedures for oral, electronic, and written consent	
s.6(2)(a)(v)	Policies for the use of personal information in artificial intelligence systems, the creation of data derived from personal information, and the creation of non-personal data	
s.6(2)(b)	Written administrative, technical, and physical safeguards for personal information, data derived from personal information, and non-personal data	

Other POPA requirements addressed by the County's PMP

Statute/Regulation	Requirement	County Document(s)
POPA s.25(3)	PMP availability to any person on request within 30 business days.	
M-Reg 143/2025 s. 6(3)	Process for making the PMP available, or publication of the PMP available on the public body's website	
M-Reg 143/2025 s.6(4)	Authority to withhold technical/security information that could compromise security	
POPA s.10	Duty to protect personal information; breach notification on real risk of significant harm	
POPA s.57	Personal Information Banks directory	
POPA Part 3	Data matching and creation of non-personal data	
M-Reg 143/2025 s.4	Real risk of significant harm determination	
M-Reg 143/2025 s.3(2)	Human oversight, auditing, and validation processes for systems creating data derived from personal information or non-personal data	
Reg 132/2025 s.1	Definitions of administrative, physical and technical safeguards	