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:	Chief Administrative Officer (CAO)
Next Review:	July 2027
Classification:	Public Document

TABLE OF CONTENTS

1. PURPOSE AND SCOPE

1.1 Purpose:

Parkland County is committed to protecting the privacy of all individuals whose personal information is collected, used or disclosed or stored by our municipality. This Privacy Management Program (PMP) is to establish pursuant to section 25 of Alberta's *Protection of Privacy Act (POPA)* and the *Protection of Privacy (Ministerial) Regulation (M-Reg 143.2025).*

The Privacy Management Program (PMP) provides a comprehensive governance framework to ensure legislative compliance, accountability, and continuous improvement in the management of personal information, Senior Leadership affirms that privacy protection is a legal obligation and an organizational priority, proportionate to the volume and sensitivity of personal information under Parkland County's custody or control.

This Privacy Management Program (PMP) outlines the governance structure, policies, safeguards and operational procedures implemented to:

1. Promote accountability by establishing clear roles, responsibilities, and processes for managing privacy risks.
2. Foster trust with our residents, employees, and partners by demonstrating a commitment to privacy.
3. Specify safeguards to protect personal information, data derived from personal information and non-personal.
4. Enable risk management tools to identify, assess, and mitigate privacy risks proactively.
5. Support business objectives by integrating privacy into business operations, enabling innovation while respecting individuals' rights.

This Privacy Management Program (PMP) will ensure Parkland County maintains ongoing compliance, and promote the responsible, transparent management of personal information.

1.2 Scope:

This Privacy Management Program (PMP) applies to:

- All Parkland County Employees;
- Contractors, consultants, and service providers acting on behalf of Parkland County;
- Elected officials;
- Volunteers.

It applies to all personal information, regardless of format (electronic, paper, audio, video or any other recorded form).

1.3 Privacy Management Program (PMP) Proportionality Determination

Parkland County has custody and control of personal information across multiple program areas, including employee records, financial information, regulatory enforcement records, and information relating to minors and vulnerable individuals. Based on this volume and sensitivity, Parkland County has implemented this Privacy Management Program (PMP) in accordance with sections 6(1) and 6(2) of the *Protection of Privacy (Ministerial) Regulation.*

2. DEFINITIONS

All definitions are referenced from the *Alberta Protection of Privacy Act (POPA)* or *Access to Information Act (ATIA)* or Parkland County Bylaws.

"Administrative Safeguards": are a policy, procedure or practice to manage a public body's conduct that protects the privacy of personal information, data derived from personal information and non-personal data.

"Breach": means the loss of, unauthorized access to, or unauthorized disclosure of personal information.

"Commissioner": means the Information and Privacy Commissioner appointed under the A*ccess to Information Act.*

"Data Derived from Personal Information": created by data matching and that identifies any individual whose personal information was used in the data matching.

"Electronic Record": means a record that exists at the time a request for access is made or that is routinely generated by a public body that can be any combination of texts, graphics, data, audio, pictorial or other information represented in a digital form that is created, maintained, archived, retrieved or distributed by a computer system.

"Head": the person or group of persons designated under section 98(a) of the *Access to Information Act (ATIA)* as the head of the public body.

"Personal Information": recorded information about an identifiable individual including:

- the individual's name, home or business address, home or business telephone number, home or business email address, or other contact information, except where the individual has provided the information on behalf of the individual's employer or principal in the individual's capacity as an employee or agent;
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual's age, gender identity, sex, sexual orientation, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
- information about the individual's health and health care history, including information about the individual's physical or mental health;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given, (viii) anyone else's opinions about the individual; and
- the individual's personal views or opinions, except if they are about someone else.

"Non-Personal Data": data, including data derived from personal information, that has been generated, modified or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the regulations.

"Physical safeguards": are a measure to protect a public body's physical assets, including electronic information systems, from natural and environment hazards and unauthorized intrusion.

"Privacy Impact Assessment (PIA)": means a due diligence assessment process conducted to determine how administrative practices and information systems relating to the collection, use or disclosure of personal information may affect the privacy of individuals. The PIA process anticipates potential privacy risks inherent

in any service delivery including in-person, post mail, telecommunications and electronic services provided through technology.

"Privacy Management Program (PMP)": means a privacy management program established and implemented under section 25 of the *Protection of Privacy Act (POPA).*

"Real Risk of Significant Harm (RROSH)": whether there exists a real risk of significant harm to an individual as a result of the loss of, unauthorized access to or unauthorized disclosure of personal information, a public body must consider each of the following factors, in addition to any other relevant factors:

(a) whether there is a reasonable basis to believe that the personal information has been misused or will be misused;

(b) whether the loss of, unauthorized access to or unauthorized disclosure of the personal information occurred as a result of malicious intent;

(c) the sensitivity of the personal information that was lost or accessed or disclosed without authorization;

(d) mitigating measures taken or other factors that reduce the risk of significant harm.

"Technical safeguards": are a measure to protect a public body's electronic information and control access to it.

3. GOVERNANCE & ACCOUNTABILITY

3.1 Head of the Public Body- Chief Administrative Officer (CAO)

Role of the Head

Responsible for ensuring compliance designated under *section 98(a) of the Access to Information Act (ATIA)* as the head of the public body. The Head may delegate authority in writing. The CAO will also receive annual reports on the effectiveness of the Privacy Management Program (PMP), including training completion rates privacy incidents, complaints and identified risks. The CAO will also ensure adequate financial and technical resources are allocated for privacy governance.

The head of a public body may delegate to any person any power, duty of function of the head under the *Access to Information Act (ATIA)* and *Protection of Privacy Act (POPA).*

3.2 Legal Services Coordinator (Privacy Officer)

Email: ATI@parklandcounty.com
Phone number: 780-968-3229

The Legal Services Coordinator is the primary point of contact for privacy compliance and access to information requests as delegated under section 55(1) of the *Protection of Privacy Act* and section 87(1) of the *Access to Information Act.*

Responsible For:

- Oversight and maintenance of this Privacy Management Program (PMP);
- Privacy Impact Assessments (PIA's);
- Privacy incident and breach response;
- Organizational training and awareness;
- Liaison with the Office of the Information and Privacy Commissioner (OIPC);
- Work with departments to ensure personal information is protected;
- Respond to requests for the correction of an individual's personal information;
- Investigate and respond to privacy incidents or complaints;
- Report material privacy risks and systemic issues to the CAO and senior leadership; and
- Maintaining the Personal Information Inventory and Personal Information Bank.

3.3 Senior Leadership Team (SLT)

Responsible for:

- Support privacy as an organizational priority;
- Provide executive oversight; and
- Ensure adequate resources will be allocated to the Privacy Management Program (PMP).

3.4 Chief Information Officer (CIO)

Responsible for:

- Oversee the implementation and maintenance of cybersecurity controls; and
- Issue and update cybersecurity directives, policies or procedures to ensure continued relevance and compliance.

3.5 Technology and Digital Services (TDS)

Responsible for:

- Conduct day-to-day cybersecurity operations;
- Coordinate cybersecurity incident response;
- Advise departments, project teams and vendors on cybersecurity arrangements;

- Serve as the primary point of contact for staff and stakeholders seeking cybersecurity guidance or reporting cybersecurity incidents; and
- Manage the Security Threat and Risk Assessment (STRA) process to ensure the organization applies the appropriate level of security based on each system, situation, or opportunity.

3.6 All County Employees

Responsible for:

- Handle personal information only as required for authorized job duties;
- Comply with all privacy policies, procedures, safeguards and training requirements;
- Immediately report suspected privacy incidents or unauthorized access to the Legal Services Coordinator; and
- Maintain confidentiality during and after employment.

3.7 Contractors

Responsible for:

- Handle personal information only as required for authorized job duties;
- Comply with all privacy policies, procedures, safeguards and training requirements;
- Immediately report suspected privacy incidents or unauthorized access to the Legal Services Coordinator; and
- Maintain confidentiality during and after contracted terms.

4. RELEVANT BYLAWS

4.1 Access to Information Bylaw 2025-28
A Bylaw to designate a person as the Head for Parkland County for the purposes of the Access to Information Act and to set fees thereunder.

4.2 Protection of Privacy Bylaw 2025-29
A Bylaw to designate a person as the head for Parkland County for the purposes of the Protection of Privacy Act, to establish a directory of Personal Information Banks and to establish a Privacy Management Program (PMP).

4.3 Records Management Bylaw 2026-19
A Bylaw to regulate the management of municipal records in accordance with the Access to Information Act, The Protection of Privacy Act and the Municipal Government Act.

Parkland County Bylaws can be found here:
https://www.parklandcounty.com/home-property-utilities/bylaws/frequently-requested-bylaws/

5. RELEVANT POLICIES, PROCEDURES AND DIRECTIVES

Parkland County maintains the following policies and procedures:

5.1 Protection of Privacy Policy C-459

To support Parkland County's Privacy Management Program by establishing clear expectations for how Personal Information is handled and protected in accordance with the *Access to Information Act (ATIA)* and *Protection of Privacy Act (POPA)*. This policy will set the criteria in determining the severity level of a privacy breach and establish the rules for investigating, documenting, and reporting privacy breaches. This policy establishes a framework for accountability, consistent decision making and risk management while supporting Parkland County's operational and service delivery needs. It also sets out high-level expectations for identifying, investigating, documenting, and responding to privacy breaches, including determining the level of risk associated with a breach.

5.2 Routine Release Directive

To establish the standards by which Parkland County will routinely release information to the public.

PLEASE NOTE: All of Parkland County's procedures, policies and directives are in the process of being reviewed and updated to reflect the changes to Alberta's Privacy & Access legislation.

6. PRIVACY IMPACT ASSESSMENTS (PIA's)

6.1 What is a Privacy Impact Assessment?

A Privacy Impact Assessment (PIA) is a process used to identify and manage privacy risks when a new program, system, or initiative, or significant changes are made to existing ones. It helps Parkland County understand what personal information is being collected, how it will be used, stored, and shared, and whether those practices are necessary and appropriate. Through this process, we ensure that privacy protections are built in from the start, risks are minimized, and we comply with applicable privacy laws and best practices.

Parkland County will conduct Privacy Impact Assessments (PIA's) to identify, assess and mitigate any privacy risks associated with new or substantially changed programs, services, systems or administrative practices. Privacy Impact Assessments support protective compliance with the Protection of Privacy Act and ensure privacy considerations are integrated into all decision making at the earliest possible stage. A Privacy Impact Assessment will be conducted where required under the *Protection of Privacy Act (POPA)*, including:

- Introducing a new program or service involving personal information;
- Implementing or significantly modifying an existing information system;
- Entering into new information sharing agreements; and
- Expanding surveillance or monitoring activities at Parkland County sites.

All PIA's will use the authorized template to ensure a comprehensive and standard format. Program areas will be responsible for consulting the Legal Services Coordinator to determine whether a PIA will be required.

6.2 Roles & Responsibilities

- Program area will initiate the Privacy Impact Assessment;
- Legal Services Coordinator will provide guidance, review the assessment to determine if the Privacy Impact Assessment will be submitted to the Office of the Information and Privacy Commissioner (OIPC) as required by the Act; and
- Senior leadership to review and approve as required by the Act.

7. PERSONAL INFORMATION INVENTORY

7.1 What is a Personal Information Inventory?

It captures all recorded personal information that is in the custody or control of a public body. This personal information includes unique identifiers, biometrics, data, or meta-data, when combined with other data, reasonably could identify an individual. Identifying the sensitivity and categories or this information is a prerequisite for the mandatory training of employees. Documenting this inventory helps maintain effective oversight and ensure Parkland County's internal policies and managing privacy incidents are grounded in an accurate map of the organization's data landscape.

Parkland County will maintain a Personal Information Inventory covering all recorded personal information under its custody or control, including information held by third-party services providers.

The Personal Information Inventory:

- Identifies categories of personal information collected, used, disclosed and retained;
- Identifies categories of individuals (e.g. residents, employees, minors, vulnerable individuals);
- Documents purposes, legal authority, storage locations (physical and electronic) and retention periods;
- Identifies whether information is shared internally, externally, or with service provides; and
- Supports the County's classification system, safeguards, training requirements and privacy impact assessments.

8. PERSONAL INFORMATION BANK (PIB)

8.1 What is a Personal Information Bank?

A personal information bank (PIB) is a way to describe the types of personal information our organization holds about individuals in our programs and services. It does not contain anyone's personal records but instead provides a general summary of what information is collected, who it relates to, why it is collected, how it is used or shared, and the legal authority for collecting it. Personal information banks help Parkland County be transparent about our information practices and allow residents to better understand how their personal information is handled and protected.

Parkland County will maintain an up-to-date inventory of a Personal Information Bank for all personal information under its custody or control. The PIB will identify the legal authority for collection, the purpose of collection and the categories of personal information involved. It will also identify the routine uses and disclosures, retention and disposal standards as well as the safeguards in place to protect the information.

The Legal Services Coordinator will conduct a formal review of the PIB on an annual basis to ensure accuracy, capture updates and ensure legislative compliance. This review will include consultation with program areas to reflect any operational changes, new initiatives or amendments to the information collected.

9. NON-PERSONAL DATA MANAGEMENT

Where Parkland County creates, uses or discloses non-personal data (including anonymized, de-identified, synthetic or data derived from personal information), the County will manage such data in accordance with the *Protection of Privacy Act (POPA).*

The County will:

- Document the personal information used to create non-personal data;
- Define the purpose and legal authority for creating the data;
- Apply de-identification methods designed to prevent re-identification;
- Conduct data quality assurance and re-identification risk assessments;
- Maintain auditability of methods and datasets; and
- Consider and mitigate potential bias in datasets.

10. AUTOMATED DECISION MAKING, ARTIFICIAL INTELLIGENCE & DATA MATCHING

10.1 Current Status

Parkland County does not currently use personal information in automated decision-making systems, Artificial Intelligence (AI) tools, or data matching activities.

10.2 Future Use

Any future use of AI with respect to decision making, automated systems or data matching will require prior authorization, completion of a Privacy Impact Assessment, transparency to individuals and human oversight, in compliance with the *Protection of Privacy Act (POPA)* part 3 and the Ministerial Regulation and organizational policies.

Where such systems are used:

- Privacy Impact Assessments (PIA's) will be completed prior to implementation;
- Individuals will be notified by collection notices when automated process is used to make decisions about them;
- Human oversight will be maintained;
- Systems will be monitored for bias, fairness and privacy risks;
- Data matching activities will comply with Part 3 of the *Protection of Privacy Act (POPA)* and all applicable regulations; and
- A Security Threat and Risk Assessment (STRA) will be used when appropriate.

11. CONSENT MANAGEMENT

Collection Notice

A collection notice is a short statement included in our forms (usually at the bottom), that explains why we are collecting your personal information. It also tells you how we will use the information and the legal authority that allows us to collect it. It also provides the contact information if you have questions about how your personal information is being handled. Collection notices help ensure transparency and allow you to make informed decisions when providing your personal information.

Where consent is required for the collection, use or disclosure of personal information, Parkland County will ensure that consent is informed, meaningful and documented.

Consent may be obtained orally, electronically or in writing and will:

- Be clearly identified in plain language;
- Be appropriate to the sensitivity of the information; and
- Be recorded where required to demonstrate compliance.

12. SERVICE PROVIDER & VENDOR OVERSIGHT

Parkland County remains accountable for personal information handled by service providers.

The County will:

- Include privacy and security requirements in contracts;
- Assess service providers' safeguards prior to engagement;
- Conduct periodic reviews or audits where appropriate; and
- Require incident notification without unreasonable delay.

13. PRIVACY COMPLAINT PROCESS

Parkland County is committed to addressing privacy complaints in a timely, fair, and transparent manner. Any individual who believes their personal information has been collected, used, disclosed, or retained improperly or contrary to the *Protection of Privacy Act (POPA)* may submit a privacy complaint.

Privacy complaints must be submitted in writing and may be directed to the Legal Services Coordinator or submitted through Parkland County's website via the designated privacy complaint form. Individuals may choose to submit a complaint anonymously. While anonymous complaints will be received, reviewed, and investigated in accordance with applicable privacy requirements under Parkland County's Privacy Management Program, no follow-up communication can be provided where contact information is not supplied.

The complaint should include sufficient detail to allow Parkland County to understand the concern and conduct a meaningful review.

Upon receipt of a privacy complaint, the Legal Services Coordinator will:

1. Acknowledge receipt of the complaint (where contact information is provided);
2. Assess the nature and scope of the concern;
3. Conduct an impartial review of relevant records, practices, and employee actions;
4. Consult with relevant program areas as required;
5. Determine whether Parkland County complied with the *Protection of Privacy Act (POPA)* and internal policies, directives and procedures;
6. Where warranted, consult the CAO and/or senior leadership; and
7. Identify corrective actions or mitigation measures where appropriate.

The Legal Services Coordinator will provide a written response outlining the findings of the review and any actions taken or recommended, where contact information is available. Where appropriate, improvements to policies, directives, procedures, or training will be implemented to prevent reoccurrence.

Any individual who is unsatisfied with Parkland County's response has the right to make a complaint to the *Office of the Information and Privacy Commissioner of Alberta (OIPC).*

14. CORRECTION OF PERSONAL INFORMATION

An individual who believes there is an error or omission of their personal information held by Parkland County may request a correction in accordance with the *Protection of Privacy Act (POPA).*

Requests for correction must be submitted in writing and provide the following:

1. Sufficient detail to identify the record in question; and
2. The correction sought, along with any supporting documentation where appropriate.

Upon receipt of a correction request, the Legal Services Coordinator will:

1. Confirm the identity of the applicant;
2. Review the record and consult with the responsible program area;
3. Determine whether the information is inaccurate or incomplete; and
4. Decide whether a correction will be made.

Where a correction is approved, Parkland County will:

1. Correct the personal information as appropriate; and
2. Notify any third parties to whom the information was disclosed, if appropriate.

If Parkland County refuses to make the requested correction, the individual will be notified in writing and advised of their right to make a complaint to the *Office of the Information and Privacy Commissioner of Alberta (OIPC)*.

15. SAFEGUARDS

Parkland County implements reasonable administrative, physical and technical safeguards to protect all information in its custody or control. Safeguards are proportionate to the sensitivity of the information and the risks associated with its collection, use, disclosure, storage and disposal. Safeguards are regularly reviewed and updated to address evolving risks, operational changes and technological updates.

15. 1 Administrative Safeguards

Administrative safeguards include policies, directives, procedures and practices that govern how personal information is handled. These include:

- A designated Privacy Officer (Legal Services Coordinator);
- Mandatory privacy training;
- Role-based access controls for all records;
- Confidentiality agreements;
- Privacy Impact Assessments (PIA's);
- Privacy breach and incident response protocols;
- Record retention and secure destruction of records;
- Vendor clauses requiring the *Protection of Privacy ACT (POPA)* compliance;
- Data sharing Agreements; and
- Mandatory Cybersecurity training for staff.

15.2 Physical Safeguards

Physical safeguards protect Parkland County facilities and physical records from unauthorized access, loss or damage. These include:

- Restricted access to Parkland County's buildings and secure areas;
- Locked filing cabinets and controlled access to the records room;
- Visitor sign in procedures;
- Surveillance systems;
- Clean desk practices; and
- Secure shredding of paper records containing personal information.

15.3 Technical Safeguards

Technical safeguards protect electronic information systems and control access to digital records. These include:

- User authentication and strong password requirements;
- Multi-factor authentication;
- Role-based system access controls;
- Firewalls, detection, prevention systems, malware monitoring;
- Secure remote access;
- System logging and monitoring;
- Backup recovery procedures; and
- Secure disposal of electronic media.

Safeguards are subject to periodic review to ensure effectiveness and alignment with all legislative requirements. All findings are reported through the appropriate channels, and corrective measures are implemented when necessary. Parkland County may conduct the following:

- Security threat assessments;
- Internal audits;
- Compliance reviews; and
- Privacy Risk Assessments.

16. CLASSIFICATION FRAMEWORK

Parkland County has adopted a security classification framework that applies to all information based on sensitivity and risk, including personal information, derived data, and non-personal data under its custody or control. The County is actively implementing this framework by reviewing and reclassifying existing processes and information assets to align with the established standards. Safeguards are being updated accordingly to ensure that higher levels of protection are consistently applied to highly sensitive information.

There are four types of document classifications:

1. Public

Information that can be freely shared with all departments or with the public with no risk.
Examples: Published material, website, public communications.

2. Protected A- Low Sensitivity

Information with low sensitivity where unauthorized disclosure would cause minimal harm. Documents can be routine internal or may contain limited personal information.
Examples: Routine correspondence, low risk administrative records.

3. Protected B- Medium Sensitivity

Information where unauthorized disclosure could cause significant harm to an individual or the organization. This classification would contain personal information and operational data requiring a higher level of protection.
Examples: Investigation records, financial information.

4. Protected C- Highly Confidential

Information with the highest sensitivity where unauthorized disclosure could cause severe harm. This classification would contain highly sensitive personal, legal or security-related information requiring the strongest safeguards.
Examples: Personnel files, legal files

17. CYBERSECURITY

Parkland County is committed to ensuring the protection of the County's digital services and infrastructure from threats through consistent security practices, effective risk management and alignment with applicable legislation, regulations and standards.

Cybersecurity is a shared responsibility across our organization. Cybersecurity responsibilities are assigned based on the role each area plays in managing and protecting County information and systems.

Technology and Digital Services, under the oversight of the Chief Information Officer, will proactively monitor information systems containing personal information, including access controls, system logs, and threat indicators. Security Threat and Risk Assessments (STRA's) will be conducted where new systems, technologies, or significant changes present heighted privacy or security risks.

18. PRIVACY BREACH & INCIDENT RESPONSE PROTOCOLS

Parkland County maintains documented policies to respond to privacy breaches. All employees must immediately report suspected breaches to the Legal Services Coordinator. Parkland County has developed a Protection of Privacy Policy.

18.1 Incident Reporting

1. All elected officials are expected to report a privacy breach or suspected privacy breach to the Chief Administrative Officer (CAO).
2. All employees are expected to report a privacy breach to the Legal Services Coordinator, as soon as it has been discovered.
3. The level of seriousness of a reported breach will be determined by the Legal Services Coordinator and may be reported to the CAO based on the following:

> **Low level breach-** disclosure of basic personal information such as name and address of an individual.
>
> **Medium level breach**- disclosure of sensitive personal information such as employment, legal, financial or minor health information of a single individual.
>
> **High level breach**- disclosure of comprehensive, detailed personal information such as bank account information, medical history, social insurance numbers, and payroll records about an individual or a group of individuals.

18.2 Real Risk of Significant Harm (RROSH)

When a privacy incident occurs, the Legal Services Coordinator will assess whether there is a real risk of significant harm by considering the sensitivity of the information, the likelihood of misuse, whether malicious intent is suspected, and any mitigating measures taken.

Breaches of Privacy obligations may result in corrective action, up to and including discipline, termination or employment or termination of contracts, in accordance with applicable legislation, policies and agreements.

18.3 Breach Incident Register

The Legal Services Coordinator maintains a Privacy Breach Incident Register documenting:

- Date of discovery;
- Description of the incident;
- Personal information involved;
- Number of individuals affected;
- RROSH determination; and
- Notifications and remediation.

Parkland County will periodically test privacy incident response procedures, including tabletop exercises to ensure staff understand escalation processes and notification obligations. The Breach Notification Log will be summarized and provided to Senior Leadership to review annually.

19. RECORDS MANAGEMENT

Parkland County recognizes that effective records management is essential to privacy protection, accountability and compliance with the *Protection of Privacy Act (POPA)* and *Access to Information Act (ATIA)*. All personal Information is retained and disposed of in accordance with Parkland County's Record Management Bylaw and approved Record Retention and Disposition Schedule. Our retention schedule is compliant with operational and statutory requirements.

Parkland County ensures:

- Personal information is retained only as long as necessary; and
- Secure Destruction methods are used.

All program areas are responsible for the management of their records.

When records containing personal information reach the end of their retention period, they are destroyed in a secure manner to prevent unauthorized access. All records are securely shredded under a secure destruction contract.

When records are subject to an access to information request, investigation, or litigation, their destruction is immediately suspended. These records are retained until the matter is resolved and the applicable retention period has elapsed, after which they may be destroyed.

20. TRAINING & EDUCATION

In accordance with the *Protection of Privacy Act (POPA)*, Parkland County will establish and maintain a training and awareness program as a part of its Privacy Management Program to support legislative compliance and the protection of personal information.

All employees will receive privacy and access to information training appropriate to their roles & responsibilities, and level of access to records or personal information.

New Employees

All new employees as of April 2026, whose duties involve the creation, collection, use, disclosure, management or storage of records or personal information are required to complete mandatory privacy and access to information training as a part of onboarding. This online training is offered by the Government of Alberta. This training will provide a foundational knowledge of the *Protection of Privacy Act (POPA)* and *Access to Information Act (ATIA*) as well as any employee responsibilities for protecting personal information. Completion of onboarding training will be documented and monitored for compliance by Employee Services.

Current Employees

All current employees whose duties involve the creation, collection, use, disclosure, management or storage of records or personal information are required to complete mandatory annual privacy training. This training will maintain awareness of legislative obligations, policy updates and emerging privacy risks. Annual training will be tailored, where appropriate, to departmental functions and risk exposure. This training is developed and delivered by the Legal Services Coordinator.

Field Staff

Field staff, whose duties do not involve the creation, handling, retention or access to information containing personal information, are not required to complete the formal privacy and access training. Where field staff may incidentally encounter personal information, they will receive targeted guidance proportionate to their role and operational duties. Legal services will support supervisors in providing guidance.

Training Objectives:

- Ensure all employees understand their obligations under the *Protection of Privacy Act (POPA)* and *Access to Information Act (ATIA);*
- Reduce the risks of privacy incidents, breaches and unauthorized exposures;
- Promote consistent and ethical handling of personal information;
- Reinforce accountability across all levels of the organization;
- Maintain awareness of emerging privacy risks, trends and best practice.

Core Training Components:

- Privacy principles and legislative requirements under *Protection of Privacy Act (POPA)* and *Access to Information Act (ATIA);*
- Identification and reporting of privacy incidents;
- Proper records handling, storage, retention, and secure destruction;
- Appropriate use and disclosure of information;
- Email and communication best practices; and
- Role-specific scenarios and risk-based guidance.

21. ONGOING ASSESSMENT AND REVISION

This Privacy Management Program (PMP) will be reviewed annually. The Legal Services Coordinator will report on the Privacy Management Program (PMP) performance, including incidents, complaints, training compliance, Privacy Impact Assessments and risk trends to Senior Leadership annually. Findings from audits, monitoring, complaints, incidents, and system changes will be used to update the Privacy Management Program (PMP) supporting continuous improvement and accountability.

Parkland County is committed to:

1. Maintaining a culture of privacy ;
2. Monitoring best practices;
3. Updating policies as legislation evolves;
4. Engaging Technology & Digital Services (TDS), Human Resources (HR) and all relevant departments with respect to privacy planning; and
5. Ensuring privacy is integrated into all municipal operations.

22. AVAILABILITY TO THE PUBLIC

As required by the *Protection of Privacy Act (POPA*):

1. Any person may request a copy of the Privacy Management Program (PMP);
2. The municipality will provide it within 30 business days; and
3. Parkland County's Privacy Management Program (PMP) is published on our website (www.parklandcounty.com).

Parkland County may withhold or redact information from the publicly available Privacy Management Program (PMP) where disclosure could compromise the security of personal information, in accordance with the *Protection of Privacy Act (POPA)* and its regulations.

Parkland County's Privacy Management Program (PMP) meets all core and enhanced requirements under M-Reg 143/2025, including the designation of a Privacy Officer, breach response procedures, Privacy Impact Assessments, safeguards, service provider management, AI governance and public availability.

23. RESOURCES

Protection of Privacy Act (POPA)
https://kings-printer.alberta.ca/1266.cfm?page=p28p5.cfm&leg_type=Acts&isbncln=9780779859061

POPA Resources
https://www.alberta.ca/popa-resources

Access to Information Act (ATIA)
https://kings-printer.alberta.ca/1266.cfm?page=a01p4.cfm&leg_type=Acts&isbncln=9780779853786

ATIA Resources
https://www.alberta.ca/atia-resources-for-public-bodies

Office of the Information and Privacy Commissioner of Alberta
https://oipc.ab.ca/

24. APPROVAL

Chief Administrative Officer (CAO)

Name: Laura Swain

Signature: _____

Date: Jun 8, 2026

Legal Services Coordinator

Name: Stephanie Harris

Signature: Stephanie Harris (Jun 8, 2026 14:06:50 MDT)

Date: Jun 8, 2026