AGENDA

Special Meeting
June 10, 2026
Immediately following the Committee of the Whole Meeting

---

1. CALL TO ORDER

2. CHANGES TO AGENDA & ADOPTION OF AGENDA

3. REQUESTS FOR DECISION

3.1 Privacy and Access Policy AD 1035-01

3.2 Access to Information Bylaw No. 1379-26

3.3 Protection of Privacy Bylaw No. 1380-26

4. CLOSED SESSION

5. OPEN SESSION

6. MOTIONS ARISING OUT OF THE CLOSED SESSION

7. ADJOURNMENT

Council Request for Decision (RFD)

Title: Privacy and Access Policy AD 1035-01

Meeting Date: 06/10/2026 **Department:** Office of the CAO

Recommendation:

THAT County Council moves to approve Policy AD 1035-01, Privacy and Access.

Background: ☐ See Appendix

On June 11, 2025, the Government of Alberta repealed the Freedom of Information and Protection of Privacy Act (FOIP) and replaced it with two separate statutes: the Access to Information Act (ATIA) and the Protection of Privacy Act (POPA). These Acts apply to all public bodies in Alberta, including municipalities, and establish a renewed legislative framework governing access to records and the protection of personal information.

Legislative Guidance:

☑ Provincial ☐ Municipal ☐ None

Details:

Protection of Privacy Act, SA 2024, cP-28.5
Access to Information Act, SA 2024, cA-1.4

Council Priorities Chart:

☐ Yes ☐ No

Details:

Previous Council Direction:

N/A

Financial Implications:

☐ Capital ☐ Operations ☐ Other

Details:

N/A

Communication and Engagement:

If Council passes the policy it will be shared with staff and updated in our files and added to the Privacy Management Program.

Implementation Timeline:

Upon passing of the Policy

Attachments: Draft Privacy and Access Policy.

Prepared By: Pat Podoborozny **Reviewed By:** Pat Podoborozny

Policy

Privacy and Access

Policy Number: AD 1035-01

Supersedes Policy Number: New

Approved by Council: TBD **Next Review Date:** June 2030

Resolution No: TBD **Last Review Date:** June 2026

POLICY STATEMENT

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. County of Minburn No 27 (County) is bound by the requirements of the *Protection of Privacy Act* (POPA) and collects, uses, and discloses personal information in accordance with its provisions. This policy establishes the principles and processes for managing County information in compliance with ATIA and POPA.

PURPOSE

The purpose of this Policy is to provide guidance and direction with respect to the County's adherence to and compliance with Privacy Legislation, and to establish principles and quality assurance standards to guide the establishment, implementation, and maintenance of the Privacy Management Program.

SCOPE

This policy applies to:

a) All County of Minburn employees, council, employees, contractors or any person acting on behalf of the municipality who collect, use or manage Personal Information in the custody or control of the County;

b) All recorded information, in whatever form or medium (paper, digital, audio-visual, graphic) created or received in the course of carrying out the County's mandated functions and activities; and

c) All facilities and equipment required to collect, manipulate, transport, transmit, or keep County information.

DEFINITIONS

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

Artificial Intelligence Service (AI Service) means 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.

Authorized Representative means 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:

- An executor or administrator of the estate of an individual who is deceased, for purposes of administering the estate
- A guardian or trustee of a dependent adult, according to appointment under law
- An agent under a personal directive, in accordance with the directive
- An individual who is acting under specific provisions of a power of attorney
- 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 (Appendix 7) of the minor
- An individual acting with the written authorization of an individual

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

CAO means the Chief Administrative Officer.

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

Common or integrated service or program means a program or service planned, administered, delivered, managed, monitored or evaluated by the County working collaboratively with one or more other public bodies or another service provider working on behalf of the County.

Confidentiality means 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.

Consent means informed agreement by an individual to the use or disclosure of their own personal information held by the County which can be revoked by the individual at any time.

Control means the responsibility and accountability for making decisions about the handling of information, regardless of whether the County has custody of the information. The County 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.

Council means the Reeve and Councillors as a whole, duly elected in the County that hold office at that time.

County means the County of Minburn No. 27.

Custody means the physical possession of information.

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

Data Matching means the linking of personal information between two or more databases or other electronic sources of information.

Disclosure means giving access to or making the personal information in the County's custody or control available to a person or organization external to the County.

Employee means an individual employed to work on a permanent, non-permanent or term basis including board members, directors, officers, contractors, students, and volunteers providing services on behalf of the County.

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

Mature Minor means 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.

Notification means an explanation of policies, procedures, consequences, and risks related to the collection, use or disclosure of an individual’s personal or personal employee information. The County 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 the County if an individual has questions about the management of their personal information.

Non-personal Data means 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.

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

Personal Information means recorded information about an identifiable individual (name, home or business address, home or business telephone number, home or

business email address, or other contact information, 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 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, anyone else's opinion about the individual, and the individual's personal views or opinions, except if they are about someone else).

Personal Information Bank (PIB) means an information repository that is organized or retrievable by an individual's name or other identifier.

Privacy Impact Assessment (PIA) means 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 the County. 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.

Privacy Management Program (PMP) means a Privacy Management Program established and implemented under Section 25 of the Protection of Privacy Act (POPA)

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

Record means 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.

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

Significant Harm means harm that results from the unauthorized access, disclosure, or loss of personal information (bodily harm, humiliation, damage to reputation or relationships, loss of employment or business or professional opportunities, identity theft, diminished insurability, diminished credit, loss of property or legal status, and loss of finances).

Third Party means 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 the County.

Use means use of information by County employees for an authorized purpose that is authorized by policy or law.

Words and phrases used in this Policy that are not defined above have the meanings given to them in Privacy Legislation.

GUIDELINES

1. Goals and Principles

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

a) Program Accountability

The County designates the CAO who is accountable for implementing and maintaining access to information and privacy for information under the custody or control of the County.

b) Openness and Transparency

The County develops and follows access, privacy, and security policies and procedures that are compliant with Privacy Legislation. With limited exceptions as provided for in Privacy Legislation, these are publicly available on the County's website.

c) Collection of Personal Information

The County 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 Process

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) Correction of Personal Information

The County makes all reasonable efforts to ensure that general information and personal information created or received by the County 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 County of Minburn custody or control, subject to limited and specific exceptions.

h) Safeguards

The County 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. Such arrangements are set out in the Information Security Policy (AD 1026-01) and the Information Management Policy (AD 1028-01). Making the details of these security arrangements public could compromise the security of the personal information, and so that information will be withheld and not made publicly available on the County's website.

i) Compliance Challenges

Individuals are encouraged to bring any concerns or issues regarding privacy and access at the County 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 the County right of access or correction responses, or any policies or practices they feel are not in compliance with legislative requirements.

j) Privacy Incidents

If any Employee becomes aware of an incident that involves the loss of, unauthorized access to, or unauthorized disclosure of personal information in the custody or under the control of the County, then the Employee will immediately notify the Privacy and Access Officer and adhere to the Privacy Breach Response Procedure. Upon notification from an Employee, or the Privacy and Access Officer otherwise becoming aware of the occurrence of an such incident, the Privacy and Access Officer will give notice, without unreasonable delay, of the incident in accordance with Privacy Legislation and the Privacy Response Procedure.

k) Data Matching, Data Derived from Personal Information, and Non-Personal Data Management

The County may carry out data matching only as allowed by and in accordance with Privacy Legislation. More specifically:

- the County may only carry out data matching to create data derived from personal information for one or more of the following purposes:
  - research and analysis;
  - planning, administering, delivering, managing, monitoring, or evaluating a program or service; or
  - one or more purposes prescribed in Privacy Legislation;
- for the purposes of data matching, the County:
  - does not collect personal information directly from an individual;
  - collects personal information from another public body;
  - may use personal information in its custody or under its control; and

- the County discloses data derived from personal information only to:

- the other public body from which data matched personal information was collected, for the purpose it was created;
- the Office of Statistics and Information for the purposes of the Office of Statistics and Information Act.

l) Artificial Intelligence and Automated Systems

When the County uses personal information in an automated system to generate content or make decisions, recommendations, or predictions, the County will ensure it only collects, uses, and discloses such personal information in accordance with Privacy Legislation. Until the applicable governance document is in effect, the Director, Corporate Services, must be consulted before such use is made.

m) Information Security Classification

Until such time that the County has established a governance document that establishes a security classification system for personal information, data derived from personal information, and non-personal data in its custody or under its control, the Director of Corporate Services must be consulted before assigning access to that information.

2. Quality Controls and Assurance

a) Policy Review

The governance documents that comprise the County's Privacy Management Program will be reviewed, assessed, and updated as frequently as is required to ensure they are effective and align with legislative, regulatory or County functional developments and changes at the minimum of every four years.

b) Training and Communication

All County employees are provided with regular training resources to ensure they adequately understand and can implement all aspects of the Privacy Management program.

For clarity, the definition of 'Employee' is broad and includes contractors and suppliers. Those contractors and suppliers must complete either: (1) the training required by the Privacy and Access Officer about their obligations under Privacy Legislation; or (2) both the Protection of Privacy Act for Public Bodies course and the Access to Information Act for Alberta Public Bodies course provided by the Government of Alberta. That training must be completed before such contractors and suppliers perform any service for the County, and valid training must be maintained during the performance of any service for the County. For purposes of the Privacy Management Program, the training expires and will no longer be considered valid on the date that is 4 years after completion.

c) Privacy, Access, and Security Monitoring and Assessment

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 County information are identified, monitored and assessed to determine the extent of the risk and the mitigation required.

3. Personal Information Banks

a) The County creates and maintains a directory of the personal information banks under its custody and control.

b) The personal information bank directory includes:
- the title of the personal information bank;
- the location of the personal information bank;
- a description of the types of personal information included;
- a description of the categories of individuals whose personal information is included;
- the authority for collecting the personal information;
- the purposes for which the personal information was collected or compiled; and,
- the purposes for which the personal information may be used or disclosed.

c) If personal information is used or disclosed for a purpose other than the one described in the directory, the County
- keeps a record of the purpose and connects that record to the personal information; and,
- updates the directory to include the new purpose in the next publication of the directory.

4. Privacy Impact Assessments

a) 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.

b) The introduction of, or change to, a system, program, service, project or practice is considered significant if:
- the loss of, unauthorized access to or unauthorized disclosure of the personal information involved could result in significant harm;
- it involves highly sensitive information;
- it involves personal information of a significant percentage of the County's service population;
- there is data matching of personal information with an external electronic information repository;
- it is part of a common or integrated service or program;
- the technology used is innovative; or
- the administrative, technical, or physical measures and systems being proposed represent an additional risk to the privacy of individuals.

c) Any projects or changes of such nature are reported to the Privacy and Access Officer, who is responsible for completing the PIA.

d) 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, ideally, before the project is implemented.

5. Roles and Responsibilities

a) Chief Administrative Officer

The Chief Administrative Officer is designated as the Head of the County for the purposes of Privacy Legislation pursuant to the Chief Administrative Officer Bylaw, and may delegate to any person any power, duty, or function of the Head under Privacy Legislation, except the power to delegate.

The Chief Administrative Officer is responsible for ensuring the County's compliance with Privacy Legislation and identifying the Privacy and Access Officer for the County.

b) Privacy and Access Officer (PAO)

The PAO is delegated by the Head to be responsible for the overall management and coordination of privacy, security and access to information at the County in accordance with a delegation order.

c) Council

Council is responsible for approving this Policy, adhering to Privacy Legislation, handling County information responsibly, and supporting transparency in governance. This includes assisting in responding to access requests for County information when requested by the Chief Administrative Officer or the Privacy and Access Officer and taking training as offered by the Chief Administrative Officer.

d) Department Directors

Directors are responsible for implementing privacy and security policies and procedures within their functional areas and are accountable for adherence to all policies by their employees and contracted third parties. Department Directors are responsible for:

- supporting their employee’s awareness of and training on privacy and security policies and procedures;
- implementing privacy and security standards and processes in compliance with policy as they relate to information repositories and operational functions and activities of their area;
- providing appropriate resources and facilities as needed to support the implementation of privacy and security policy in the department;
- referring all formal right of access requests for information to the PAO;
- cooperating and assisting in locating and retrieving departmental information relevant to right of access requests;
- reporting gaps in privacy, access and security policy affecting their areas to the PAO;
- reporting any new information repositories or data systems that require registration, assessment, and security classification to the PAO.

e) All County Employees and Service Providers

All County 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:

- make themselves aware of and adhere to privacy, access and security and standards;
- at the time of hire or engagement complete an oath of confidentiality;
- capture, manage, access, release and protect information in their custody or control according to privacy, access and security policy;
- access, release and protect information in their custody or control according to policy;
- refer to the PAO all decisions about collection, use, disclosure, and access that are not clearly directed by policy;
- report all suspected breaches to personal information to the PAO immediately upon discovery; and
- identify and report information security incidents to the appropriate management according to privacy breach procedures.

f) Information Technology Management

IT Management, in coordination with the PAO, for all systems, networks and applications:

- implements and deploys privacy and security measures;
- completes risk and mitigation assessments;
- monitors and detects security threats; and
- assists in the response to privacy breaches.

Council Request for Decision (RFD)

Title: Access to Information Bylaw No. 1379-26

Meeting Date: 06/10/2026 **Department:** Office of the CAO

Recommendation:

THAT County Council give first reading to Access to Information Bylaw No. 1379-26.
THAT County Council give second reading to Access to Information Bylaw No. 1379-26.
THAT County Council give consider giving unanimous consent to going to third reading to Access to Information Bylaw No. 1379-26.
THAT County Council give third reading to Access to Information Bylaw No. 1379-26.

Background: ☐ See Appendix

The Government of Alberta has modernized access and privacy legislation through the Access to Information Act which imposes clear obligations on municipalities as public bodies to provide a right of access to records in municipal custody or control, process requests in a timely consistent, and transparent manner and establish reasonable fees for certain services related to access requests.

Legislative Guidance:

☑ Provincial ☐ Municipal ☐ None

Details:

Access to Information Act, SA 2024, cA-1.4

Council Priorities Chart:

☐ Yes ☐ No

Details:

Previous Council Direction:

Council passed Bylaw No. 1142-99 Public Access to Information and FOIP on September 20, 1999.

Financial Implications:

☐ Capital ☐ Operations ☐ Other

Details:

N/A

Communication and Engagement:

If Council passes the bylaw it will be shared with staff and updated in our files and added to the Privacy Management Program.

Implementation Timeline:

Upon passing of third reading

Attachments: Draft Access to Information Bylaw No. 1379-26
Public Access to Information and FOIP Bylaw No.1142-99

Prepared By: Pat Podoborozny **Reviewed By:** Pat Podoborozny

COUNTY OF MINBURN NO. 27

BYLAW NO. 1379-26

A BYLAW OF THE COUNCIL OF THE COUNTY OF MINBURN NO. 27, VEGREVILLE, IN THE PROVINCE OF ALBERTA TO DESIGNATE A PERSON AS THE HEAD FOR THE COUNTY OF MINBURN NO. 27 FOR THE PURPOSES OF THE ACCESS TO INFORMATION ACT AND TO SET FEES THEREUNDER.

WHEREAS pursuant to Section 98(a) of the *Access to Information Act*, SA 2024, Chapter A-1.4, the County of Minburn No. 27 must designate a person or group of persons as the head of County of Minburn No. 27 for the purpose of the Act; and

WHEREAS pursuant to Section 98(b) of the *Access to Information Act,* SA 2024, Chapter A-1.4, the County of Minburn No. 27 may set any fees for the municipality requires to be paid under Section 96, which must not exceed the fees provided for the Regulation;

NOW THEREFORE the Council of the County of Minburn No. 27, in the Province of Alberta, duly assembled and under the authority of the *Municipal Government Act*, Revised Statutes of Alberta 2000, Chapter M-26, as amended, hereby enacts as follows:

Title

1. This Bylaw may be known as the "Access to Information Bylaw".

Definitions

2. The following definitions will apply to the corresponding words in this Bylaw:

   Act means the *Access to Information Act,* SA 2024, Chapter A-1.4;

   Applicant means a person who makes a request for access to a record under Section 7 of the Act;

   CAO means the Chief Administrative Officer;

   County means the County of Minburn No. 27;

   Regulations means the *Access to Information Act Regulation,* Alta Reg 133/2025.

Interpretation

3. The headings in this Bylaw are for reference purposes only.

Designated Head

4. For the purposes of the Act, the CAO is designated as the head of the County.

Fees

5. Where an Applicant is required to pay a fee for services, the fee payable is in accordance with the *Access to Information Act* and the *Regulation*, as amended from time to time, or any successor regulation that sets fees for requests to access information.

Enactment/Transition

6. Should any provision of this Bylaw be deemed invalid then such invalid provision will be severed from this Bylaw, and such severance will not affect the validity of the remaining portions of this Bylaw, except to the extent necessary to give effect to such severance.

7. Bylaw 1142-99 is hereby repealed.

Effective Date

8. This Bylaw shall come into force and effect upon third reading and signing thereof.

FIRST READING ..... _____, 2026

SECOND READING ..... _____, 2026

THIRD READING..... _____, 2026

_____
REEVE

_____
CHIEF ADMINISTRATIVE OFFICER

COUNTY OF MINBURN NO. 27

BY-LAW NO. 1142-99

A BY-LAW OF THE COUNCIL OF THE COUNTY OF MINBURN NO. 27 TO ESTABLISH ADMINISTRATIVE PROCEDURES AND FEES FOR ACCESS TO GENERAL INFORMATION AND INFORMATION IN REFERENCE TO THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY (FOIP) ACT S.A. 1994 C.F. - 18.5 AND REGULATIONS THEREUNDER INCLUDING AMENDMENTS.

WHEREAS the County provides the public access to general information or records in the possession of the County unless there is (are) reason(s) why the information should not be disclosed;

WHEREAS the Freedom of Information and Protection of Privacy Act and other federal and provincial Acts and regulations authorizes the collection, maintenance, use, disclosure and restrictions of information and records.

NOW THEREFORE the Council of the County of Minburn No. 27, in the Province of Alberta, duly assembled, hereby enacts as follows:

1. The County Manager (CAO) is designated as the Head of the County for the purposes of the Freedom of Information and Protection of Privacy Act (FOIP) and for public access to general information.

2. That the County Manager (CAO) or designate receive and respond to requests and/or applications for information or records from the public, and is responsible and accountable for all decisions made under the Freedom of Information and Protection of Privacy Act and other information requests.

3. That members of the public requesting general or FOIP information/records in the possession of the County be required, at the County Manager's (CAO) or designate's discretion, to submit an oral request or complete the appropriate Request For Information form as provided in the County Policy No. AD 14.

4. That a schedule of fees is established by Policy No. AD 14 by Council for general information and be amended from time to time, as required by resolution. The Freedom of Information and Protection of Privacy Act information fees are chargeable as set by Alberta Regulation.

5. This By-Law becomes effective October 1, 1999.

6. By-Law No. 1120-96 is hereby rescinded.
   By-Law No. 98-08 is hereby rescinded.

READ A FIRST TIME..... September 20, 1999

READ A SECOND TIME..... September 20, 1999

READ A THIRD TIME AND PASSED ..... September 20, 1999

Original Signed

SID A. HINTON: REEVE

Original Signed

DAVID MARYNOWICH
COUNTY MANAGER

Council Request for Decision (RFD)

Title: Protection of Privacy Bylaw No. 1380-26

Meeting Date: 06/10/2026 **Department:** Office of the CAO

Recommendation:

THAT County Council give first reading to Protection of Privacy Bylaw No. 1380-26.
THAT County Council give second reading to Protection of Privacy Bylaw No. 1380-26.
THAT County Council give consider giving unanimous consent to going to third reading to Protection of Privacy Bylaw No. 1380-26.
THAT County Council give third reading to Protection of Privacy Bylaw No. 1380-26.

Background: ☐ See Appendix

The Government of Alberta has modernized access and privacy legislation through the Protection of Privacy Act, which expands obligations for public bodies regarding accountability for personal information, transparency in how information is managed, breach reporting and risk mitigation, and proactive privacy program requirements Municipalities, as public bodies, must identify and document Personal Information Banks (PIBs), ensure appropriate safeguards and accountability measures, implement policies and procedures governing privacy practices.
Currently, the municipality manages personal information across multiple departments (e.g., utilities, tax, HR, protective services), but does not have a consolidated bylaw or formalized privacy management framework aligned with updated legislative standards.

Legislative Guidance:

☑ Provincial ☐ Municipal ☐ None

Details:
Protection of Privacy Act, SA 2024, cP-28.5

Council Priorities Chart:

☐ Yes ☐ No

Details:

Previous Council Direction:

None, New Bylaw

Financial Implications:

☐ Capital ☐ Operations ☐ Other

Details:
N/A

Communication and Engagement:

If Council passes the bylaw it will be shared with staff and updated in our files and added to the Privacy Management Program.

Implementation Timeline:

Upon passing of third reading

Attachments: Draft Protection of Privacy Bylaw No. 1380-26

Prepared By: Pat Podoborozny **Reviewed By:** Pat Podoborozny

COUNTY OF MINBURN NO. 27

BYLAW NO. 1380-26

A BYLAW OF THE COUNCIL OF THE COUNTY OF MINBURN NO. 27, VEGREVILLE, IN THE PROVINCE OF ALBERTA TO DESIGNATE A PERSON AS THE HEAD FOR THE COUNTY OF MINBURN NO. 27 FOR THE PURPOSES OF THE PROTECTION OF PRIVACY ACT AND TO ESTABLISH A PRIVACY MANGEMENT PROGRAM.

WHEREAS pursuant to Section 55(1) of the *Protection of Privacy Act*, SA 2024, Chapter P-28.5, the County of Minburn No. 27 may delegate to any person any power, duty of function of the head under this Act, except the power to delegate;

WHEREAS pursuant to Section 55(2) of the *Protection of Privacy Act*, SA 2024, Chapter P-28.5, a delegation under Section 55(1) must be in writing and may contain any conditions or restrictions the head of the public body considers appropriate;

WHEREAS pursuant to Section 57(2) of the *Protection of Privacy Act*, SA 2024, Chapter P-28.5, the head of the County of Minburn No 27 must publish a directory, in printed or electronic form, that lists the County of Minburn's personal information banks; and

WHEREAS pursuant to Section 6(1) of the *Protection of Privacy Act (Ministerial) Regulation*, Alta Reg 143/2025, the County of Minburn No. 27 must establish a Privacy Management Program;

NOW THEREFORE the Council of the County of Minburn No. 27, in the Province of Alberta, duly assembled and under the authority of the *Municipal Government Act*, Revised Statutes of Alberta 2000, Chapter M-26, as amended, hereby enacts as follows:

Title

1. This Bylaw may be known as the "Protection of Privacy Bylaw".

Definitions

2. The following definitions will apply to the corresponding words in this Bylaw:

   Act means the *Protection of Privacy Act,* SA 2024, Chapter P-28.5;

   CAO means the Chief Administrative Officer;

   County means the County of Minburn No. 27;

   Personal Information Bank means 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;

   Privacy Management Program means a privacy management program established and implemented under Section 25 of the Protection of Privacy Act (POPA);

   Regulation means the *Protection of Privacy Act (Ministerial) Regulation*, Alta Reg 143/2025.

Interpretation

3. The headings in this Bylaw are for reference purposes only.

Designated Head

4. For the purposes of the Act, the CAO is designated as the head of the County.

Privacy and Access Officer

5. For the purpose of the Act, the CAO is the Privacy and Access Officer unless designated to a member of the County staff.

Enactment/Transition

6. Should any provision of this Bylaw be deemed invalid then such invalid provision will be severed from this Bylaw, and such severance will not affect the validity of the remaining portions of this Bylaw, except to the extent necessary to give effect to such severance.

Effective Date

7. This Bylaw shall come into force and effect upon third reading and signing thereof.

FIRST READING ..... _____, 2026

SECOND READING ..... _____, 2026

THIRD READING..... _____, 2026

_____
REEVE

_____
CHIEF ADMINISTRATIVE OFFICER