

ACCESS TO INFORMATION & PROTECTION OF PRIVACY POLICY

FILE CODE: GENERAL GOVERNMENT SERVICES

DEPARTMENT CODE: ADMINISTRATION No. 12

DATE APPROVED: JUNE 9, 2026

MOTION NO.: 291/09/06/26

REPLACED: NEW



PHILOSOPHY

The County of Northern Lights values and respects the importance of balancing public access to information with the protection of personal information held by the County of Northern Lights and therefore establishes a **Privacy Management Program** within the scope and context of this Policy.

PURPOSE

- 1.1 To administer, recognize, and provide support to protect the personal information within the custody and control of the County and the availability of those records, subject to limited and specific exceptions set out in the *Access to Information Act* (ATIA) and *Protection of Privacy Act* (POPA).
- 1.2 To support the Head of the Public Body and the designated Access to Information and Privacy Officer by providing funding for a responsible and compliant Privacy Management Program that incorporates all County Employees, Councillors, Contractors/Vendors, and Volunteers.
- 1.3 The County is committed to complying with the *Access to Information Act* (ATIA) and the *Protection of Privacy Act* (POPA).

DEFINITIONS

- 2.1 “**ATIA**” means the *Access to Information Act Statutes of Alberta, 2025, Chapter A-1.4*; and any amendments thereto.
- 2.2 “**ATI & Privacy Officer**” shall mean the person designated and appointed by Council to hold the position of and administer the County of Northern Lights responsibilities under the *Access to Information Act* (ATIA) and *Protection of Privacy Act* (POPA).
- 2.3 “**CAO**” means the person appointed as the Chief Administrative Officer of the County of Northern Lights and includes any person who holds the position of CAO in an Acting capacity.
- 2.4 “**County**” means the County of Northern Lights.
- 2.5 “**Collection**” means the gathering, acquisition, receiving or obtaining of Personal Information, whether that information is collected through such methods as interviews, questionnaires, surveys, polling, or by completing forms. Collection may be in writing, audio or video recording, electronic data entry, Oral Consent or other such means.
- 2.6 “**Council**” means the sworn-in Elected Officials of the County of Northern Lights.

- 2.7 **“Disclosure”** means to release, transmit, reveal, expose, show, provide copies of, verbally state the contents of, or give Personal Information by any other means to someone. It includes oral transmission or information by telephone, or in person; provision of Personal Information on paper, by facsimile or in any other format; and electronic transmission through electronic mail, data transfer or internet.
- 2.8 **“Employee”** means any individual employed by the County and, for the purposes of this Policy, includes elected officials, third-party vendors, contractors, subcontractors, firefighters, and volunteers who access County information. Unless the context requires otherwise, any reference to an “Employee” in this Policy includes all such individuals, all of whom are required to comply with this Policy.
- 2.9 **“Express Consent”** means a specific authorization given by an individual in writing.
- 2.10 **“Implied Consent”** means that consent is reasonably inferred where an individual voluntarily provides personal information in circumstances where the purpose for the collection, use, or disclosure is obvious and reasonably understood. Implied consent is generally appropriate for routine County operational activities.
- 2.11 **“Non-Personal Data”** means data, including data derived from personal information that has been generated, modified, or anonymized so that it does not identify any individual.
- 2.12 **“Oral Consent”** means that the individual will verbally agree to participate. No document (consent form) is used.
- 2.13 **“Personal Information”** means recorded information about an identifiable individual.
- 2.14 **“Privacy Impact Assessment”** (PIA) means a process that describes how proposed administrative practices (services and programs) relating to the Collection, Use and Disclosure of Personal Information may affect the privacy of the individual who is the subject of the information.
- 2.15 **“Privacy Management Program”** (PMP) means and is the scope of the ATI & POP Policy. The PMP will have Procedures noted in Schedule “A” regarding program controls that promote the County’s compliance with its duties under ATIA and POPA.
- 2.16 **“POPA”** means the *Protection of Privacy Act, Statutes of Alberta, 2024 Chapter P-28.5* and any amendments thereto.
- 2.17 **“Third Party”** means any person, group, or organization that is completely separate from the two primary entities involved in an information request.
- 2.18 **“Use of Personal Information”** means employing collected information to accomplish the County’s purposes, such as using the information to administer a benefit, program, activity, or provide a service. Access to a file or database by program staff or contract agent constitutes “use” as defined under the ATIA and POPA.

GENERAL RESPONSIBILITIES

Privacy protection is a shared responsibility across all County departments, employees, contractors, and elected officials.

- 3.1 The County shall establish, maintain, and periodically review the Privacy Management Program in accordance with the *Protection of Privacy Act* and applicable regulations.
- 3.2 The CAO will ensure that accountability for privacy issues is clearly incorporated into the duties of all County employees, with:

- a. established policies and procedures
- b. training
- c. confidentiality agreements
- d. job descriptions
- e. access controls
- f. disciplinary process

3.3 Directors are responsible for ensuring that:

- a. personal information within their department is collected, used, disclosed, retained and disposed of in accordance with ATIA, POPA and County procedures
- b. employees receive appropriate privacy and security guidance
- c. privacy risks are identified and addressed within departmental programs and services
- d. privacy breaches are promptly reported, and
- e. privacy impact assessments are completed where required

3.4 All employees of the County are responsible for:

- a. accessing personal information only where necessary to perform authorized duties
- b. complying with County privacy and information security policies and procedures
- c. complete mandatory privacy and security training
- d. respecting the confidentiality of personal information and complying with the County's information control and security systems, and
- e. reporting any suspected or actual breaches of privacy to their immediate supervisor, the CAO, or the ATI & Privacy Officer

3.5 The ATI & Privacy Officer is responsible for the overall development, implementation, and monitoring of the County's Privacy Management Program. The primary responsibilities of the ATI & Privacy Officer are:

- a. managing the Access to Information request process for the County
- b. liaison for public inquiries
- c. providing advice to Directors and Council, including information that can be disclosed without an Access to Information request
- d. assists departments with respect to the management of records regarding Access to Information and Protection of Privacy responsibilities
- e. provides advisory services to County employees, including training on access to information, collection of information, and protection of privacy

3.6 Elected Officials are responsible for protecting personal information obtained through their official duties and complying with all applicable County privacy and security requirements.

ACCESS AND ACCURACY OF PERSONAL INFORMATION

The County shall:

- 4.1 Make every reasonable effort to ensure an individual's personal information in the custody and control of the County is accurate and complete;
- 4.2 Provide a person access to their own personal information subject to limited and specific legislative requirements; and
- 4.3 Make every effort to allow a person access to their own personal information to verify, update, and correct it.

CLASSIFICATION OF INFORMATION

The County shall protect personal information based on the following classifications:

- 5.1 **Classification 1 - Public** - Applies to data and information that, if compromised, will not result in injury to individuals, governments, or to private sector institutions.
- 5.2 **Classification 2 - Protected** - Applies to data and information that, if compromised, could cause injury to an individual, organization, or government.
- 5.3 **Classification 3 - Protected** - Applies to data and information that, if compromised, could cause serious injury to an individual, organization, or government.
- 5.4 **Classification 4 - Protected** - Applies to data and information that, if compromised, could cause extremely grave injury to an individual, organization, or government.

COLLECTION, USE, AND DISCLOSURE

- 6.1 Where required, consent shall be obtained through oral, electronic, express, or implied means and documented for the collection, use, and/or disclosure of personal information except when otherwise authorized by the ATIA and POPA.
- 6.2 Subject to the legal exceptions and reasonable notice, consent may be withdrawn at any time. Withdrawal of consent should be in writing, as it may result in unintended consequences, such as the inability to provide services to the individual.

EXCEPTIONS

- 6.3 There are circumstances in which the County is not required to obtain an individual's consent or provide an explanation for the purposes for the collection, use, or disclosure of their personal information. These include, but are not limited to:
 - a. Collection - The County may collect personal information without consent when it is in the individual's interest and timely consent is unavailable, or to investigate a breach of an agreement, or contravention of law.
 - b. Use - The County may use personal information without consent for similar reasons as those listed above, as well as in an emergency in which an individual's life, health, property, or security is threatened.
 - c. Disclosure - The County may disclose personal Information without consent for law enforcement security purposes, for debt collection, to a lawyer representing the County, and in emergency situations in which an individual's life, health, or security is threatened.

COLLECTION

- 6.4 Collection of personal information shall be done in a confidential manner to minimize the risk of disclosing sensitive personal information to third parties.
- 6.5 The privacy of individuals will be protected in accordance with POPA. Personal Information that is collected will adhere to Section 4 of POPA and is to be protected in accordance with the Protection and Retention Section of this Policy.
- 6.6 The County shall use and disclose an individual's personal information only:
 - a. For the purpose for which it was collected or for a use consistent with that purpose;

- b. For other purposes for which the County has consent from the individual; or
- c. For other purposes where the County is required or permitted to do so by law.

NON-PERSONAL DATA

- 6.7 The County may create, use, or disclose information derived from personal information, including statistical, analytical, or de-identified information, where measures have been taken to protect against the identification or re-identification of individuals. Prior to the use or disclosure of non-personal data, the County shall assess the risk of re-identification and implement reasonable measures to reduce the risk.
- 6.8 Derived information shall only be used for the County's administrative, operational, planning, research, reporting, or service improvement purposes.

USE AND DISCLOSURE

The County may use or disclose information for routine releases where:

- a. Disclosure is required by ATIA and POPIA
- b. The information is routinely requested
- c. The information is already publicly available, and/or
- d. No exceptions to disclosure under ATIA apply

ARTIFICIAL INTELLIGENCE

- 6.9 The County's Generative Artificial Intelligence Policy governs the use of artificial intelligence systems, and technologies that use personal information to generate content, recommendations, predictions, or decisions with appropriate privacy, security, and human oversight.
- 6.10 Any loss of personal information or inadvertent disclosure of personal information shall, whenever possible, be reported to the individual whose information has been lost or disclosed.

PRIVACY AND BREACH RESPONSE

- 7.1 The County shall assess whether a privacy breach creates a real risk of significant harm to affected individuals in accordance with POPIA and applicable regulations.
- 7.2 Any actual or suspected privacy breach involving Personal Information shall be immediately reported to the immediate supervisor, CAO or ATI & Privacy Officer.
- 7.3 The County shall take reasonable steps to:
 - a. contain the breach
 - b. assess the scope and potential risks associated with the breach
 - c. investigate the cause of the breach
 - d. mitigate potential harm; and
 - e. implement corrective measures to reduce the likelihood of recurrence
- 7.4 Where appropriate, the County may notify:
 - a. affected individuals
 - b. the Office of the Information and Privacy Commissioner of Alberta; and/or
 - c. law enforcement or other relevant authorities

- 7.5 All privacy breaches and suspected privacy breaches shall be documented and retained in accordance with County procedures and records management requirements.

PROTECTION & RETENTION

- 8.1 The County shall protect personal information by making reasonable security arrangements. The County shall establish and maintain written administrative, physical, and technical safeguards to protect personal information, derived information, and non-personal data.
- 8.2 Personal Information shall be protected from unauthorized access, use, disclosure, or destruction through a system of administrative, physical, and technical controls, including but not limited to:
- a. Restricting access to personal information that is stored in an electronic format to authorized persons by requiring login credentials
 - b. Storing personal information in locations which are not generally accessible to members of the public; and
 - c. Securing rooms and filing cabinets that contain personal information during those times in which an authorized person is not present
 - d. Implement additional technical safeguards including encryption, multi-factor authentication, network monitoring, and cybersecurity awareness training
- 8.3 Personal information that is no longer required to fulfill identified purposes will be destroyed in accordance with the County's Records Retention Bylaw.
- 8.4 If there is an ongoing investigation with the Office of the Information and Privacy Commissioner of Alberta, the records must remain intact until the investigation is considered closed by the Office of the Information and Privacy Commissioner of Alberta.

COMPLIANCE

- 9.1 Instances of possible non-compliance with the ATIA & POPIA or this Policy shall be immediately reported to the ATI & Privacy Officer for investigation.
- 9.2 Any Employee who violates this Policy may be subject to appropriate corrective action. For County employees, corrective action may include discipline, up to and including dismissal for cause. For third-party vendors, contractors, subcontractors, and volunteers, corrective action may include restrictions on access, termination of assignments, contracts, or services, notification to Council where applicable, and any other measures available to the County at law or under contract.
- 9.3 Where the non-compliance involves an Elected Official, Council will be notified in accordance with applicable County processes.

PERSONAL INFORMATION REQUESTS

- 10.1 Any written or verbal requests for access to information not part of a routine release shall be forwarded to the ATI & Privacy Officer.
- 10.2 Upon a access to information request, an individual will be informed of the existence, use and disclosure of their personal information, if such information is currently under the custody and control of the County, and may be given access to, and challenge the accuracy and completeness of that information.
- 10.3 Pursuant to the ATIA, exceptions to disclosure include, but are not limited to:

- a. Personal information about another person might be revealed; in this case, the County may redact certain information
- b. Commercially confidential information might be revealed; in this case, the County may redact certain information
- c. An individual's life or security might be threatened.
- d. The information was collected without consent for the purposes related to an investigation of a breach of an agreement or contravention of the law; or
- e. The information was generated during a formal dispute resolution process

GENERAL PUBLIC ACCESS

- 11.1 The County will continue to make general information available to the public, including current policies and procedures, by publishing them on the County website.
- 11.2 The information that the County makes publicly available will include, but is not limited to:
 - a. The contact information for the ATI & Privacy Officer
 - b. The means of gaining access to personal information held by the County
 - c. A description of the type of personal information held by the County and a general account of use.
 - d. Information that explains the County's policy and procedures

PRIVACY IMPACT ASSESSMENTS

- 12.1 The PIA process was developed by the Office of the Information and Privacy Commissioner of Alberta to assist public bodies in reviewing the impact that new projects may have on an individual's privacy. Privacy considerations should be integrated at the earliest stages of developing new programs or automated information systems to ensure they reflect the requirements of the ATIA and POPA.
- 12.2 This process is also designed for the County to evaluate existing programs and ensure compliance with the ATIA and POPA.
- 12.3 Departments conducting a PIA will use the instructions and questionnaire provided by the Office of the Information and Privacy Commissioner of Alberta, and will include:
 - a. A description of the project/program and the nature and sensitivity of the Personal Information involved
 - b. Relevant privacy principles and potential issues for the project, including recommendations to address the issues identified
 - c. A data flow analysis, including a description of the uses of the Personal Information and all consistent purposes and authorized Disclosures
 - d. Consideration of how the privacy requirements of the ATIA and POPA will be met
 - e. An overall assessment of the privacy impact (high, medium, or low), including a risk/threat analysis; and
 - f. The ATI & Privacy Officer will assist with the preparation of the PIA, including conducting the audit portion of the PIA, when required

POLICY REVIEW

- 13.1 Council will routinely review and approve any amendments to this Policy.
- 13.2 The ATI & Privacy Officer will be responsible for reviewing procedures related to this Policy and the Privacy Management Program and recommending updates where necessary.

ATTACHMENTS/SCHEDULES/APPENDIX

Schedule "A"	List of Internal County Procedures
	Government of Alberta's Privacy Impact Assessment Template and Guide

REFERENCES

Legal Authorities	<i>Municipal Government Act</i> <i>Access to Information Act</i> <i>Protection of Privacy Act</i> County of Northern Lights Records Retention Bylaw No. 14-12-336
Related Policies	
Other	

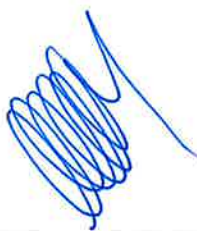
REVISION HISTORY

DOCUMENT CLASSIFICATION UNDER ATIA AND POPA

Classification 1	Public
------------------	--------



Chief Elected Official



Chief Administrative Officer

SCHEDULE “A” to ACCESS TO INFORMATION & PROTECTION OF PRIVACY POLICY

INTERNAL POLICY PROCEDURES

LIST OF INTERNAL COUNTY PROCEDURES THAT MUST ACCOMPANY THIS POLICY - SHORT WORDED AS THE **“PRIVACY MANAGEMENT PROGRAM”**.

(this list is just the beginning, no doubt more procedures will evolve over time)

Responding to Access to Information Requests

Collection and Consent of Personal Information

Security Classification System - Data and Information

Derived and Non-Personal Data

Digital Protection of Sensitive information

Generative AI Use and Approval

Physical Protection of Sensitive Information

Privacy Impact Assessment (use Government of Alberta Forms)

Personal Information Correction Request

Privacy Breach Response

Privacy Training Awareness

Responding to Privacy Complaints

Timelines for Periodic Review of Privacy Management Program