CITY OF ST. ALBERT

ADMINISTRATIVE DIRECTIVE

NUMBER	TITLE		
A-LS-07	**Privacy, Access and Security**		
DEPARTMENT		**APPROVAL DATE**	**DATE LAST REVISED**
Legal, Legislative & Records Services		June 8, 2026	N/A

Purpose

To establish the principles and processes for managing City information in compliance with the Alberta *Access to Information Act* (ATIA) and the *Protection of Privacy Act* (POPA). The ATIA ensures individual right of access to information and protects the Personal Information of the public and employees of public bodies operating in Alberta. The City is bound by the requirements of POPA and collects, uses, and discloses Personal Information in accordance with its provisions.

Directive Statement

The City is committed to the responsible management of information in accordance with access and privacy legislation. This includes safeguarding Personal Information, ensuring appropriate access to records, and maintaining strong information security practices across all City operations.

Through this directive, the Privacy, Access and Security Governance Procedures, and other relevant City administrative directives the City establishes a comprehensive Privacy Management Program that integrates privacy, access, and information security into a unified framework. The program is designed to support transparency, accountability, and public trust while enabling effective and efficient service delivery.

Scope

This directive applies to:

1. All City employees, officers, contractors, students, and volunteers providing services on behalf of the City;
2. All recorded information, in whatever form or medium (paper, digital, audio-visual, graphic) created or received while carrying out the City's mandated functions and activities; and
3. All facilities and equipment required to collect, manipulate, transport, transmit, or keep City information.

Definitions

“Access and Privacy Legislation” Alberta’s *Protection of Privacy Act* (POPA) and the *Access to Information Act* (ATIA), each as may be amended or replaced, from time to time.

“AI-Generated Content” Any material in any format that is created by or with the assistance of AI or that utilizes AI, including but not limited to text, speech, videos, and images.

“Artificial Intelligence” means technologies designed to perform tasks that typically require human intelligence, such as understanding language, analyzing data, generating content, reasoning, learning, problem-solving, perception, and decision-making through algorithms, machine learning, and natural language processing.

“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:

a) An executor or administrator of the estate of an individual who is deceased, for purposes of administering the estate.
b) A guardian or trustee of a dependent adult, according to appointment under law.
c) An agent under a personal directive, in accordance with the directive.
d) An individual who is acting under specific provisions of a power of attorney.
e) 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 **(Privacy, Access, and Security Governance Procedures Appendix 4)** of the minor.
f) An individual acting with the written authorization of an individual.

“Chief Administrative Officer” or “CAO” means the individual appointed by Council to the position of Chief Administrative Officer under section 205 of the *Municipal Government Act*.

“City” means the municipal corporation of the City of St. Albert, or where the context so requires, the area contained within the boundaries of the City of St. Albert;

“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 City working collaboratively with one or more other public bodies or another public body working on behalf of the City or the City and one or more other public bodies.

“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 this directive.

“Consent” means informed agreement by an individual to the Use or disclosure of their own Personal Information held by a public body, which can be revoked by the individual at any time.

“Control” means responsibility and accountability for making decisions about the handling of information, regardless of whether the City has Custody of the information. The City 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 municipal Council of the City of St. Albert.

“Custody” means the effective 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 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 City’s Custody or Control available to a person or organization external to the City.

“Employee” means all employees, including officers, councillors, contractors, students, and volunteers providing services on behalf of the City.

“External Networked Source” means interconnected computer networks, such as the internet, that contain information for which the City has little to no control over content creation, integrity or disclosure.

“High Sensitivity Information” means Personal Information about an individual that is:

a) Biometric information
b) Financial information
c) Personal Information about a minor, senior, or vulnerable person.

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

“Large Language Model (LLM)” means the language model of an AI that has been trained using vast amounts of data to learn patterns and language that generate human-like inferences.

“Law Enforcement” means policing, including criminal intelligence operations, security or administrative investigation that leads or could lead to a penalty or sanction.

“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 directives, procedures, consequences, and risks related to the collection, Use or disclosure of an individual’s personal or Personal

Employee Information. The City 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 City 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 information about an identifiable individual including:

a) Name
b) Address, telephone, email, or contact information*
c) Race
d) National or ethnic origin
e) Colour
f) Religion
g) Political beliefs or associations
h) Age
i) Sex
j) Marital status
k) Family status
l) Identifying numbers
m) Fingerprints or blood type
n) Educational, financial, employment, criminal records
o) Opinions about the individual
p) Individual's personal views or opinions (except opinions about others)

*Home or business address, telephone, email, or other contact information of an employee of a public body, or any individual is not Personal Information, if it is provided on behalf of the employer in the individual’s capacity as employee or agent.

Personal Information under ATIA and POPA that is not normally excepted from disclosure:

a) Opinions contained in work product.
b) Classification, salary range, discretionary benefits, or employment responsibilities of public body employees.
c) Financial and other details of a contract to supply goods or services to a public body.
d) Information about a license, permit, financial or other discretionary benefit granted to an individual by a public body.
e) Information is about an individual who has been dead for 25 years or more.
f) Information is about an individual’s enrolment at a school, attendance at a public event, or receipt of an award granted by a public body.

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

“Privacy Breach” is an unauthorized disclosure, Use, destruction, loss, removal, or modification of information in the Custody or Control of the City. Events are considered unauthorized by reference to this directive and/or access and privacy legislation. A Privacy Breach may be accidental or the result of a deliberate act.

“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 a public body. 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.

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

“Reasonable Security Arrangements” means administrative, physical and technical safeguards to protect Personal Information, data derived from Personal Information and Non-personal Data in the Custody or under the Control of the City that are appropriate and proportional with the security classification level of the information and in the case of Non-personal Data, ensure to the extent possible, that the identity of the an individual who is the subject of Non-personal Data cannot be re-identified from the data.

“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.

“Severing” means in a right of access request, separating or hiding/redacting information in a document that should or cannot be released so that the remainder of the document can be disclosed.

“Significant Harm” means harm that results from the unauthorized access, disclosure, or loss of Personal Information, including:

a) Bodily harm.
b) Humiliation.
c) Damage to reputation or relationships.
d) Loss of employment or business or professional opportunities.
e) Identify theft.
f) Diminished insurability.
g) Diminished credit.
h) Loss of property or legal status.
i) Loss of finances.

The following factors are also considered in determining the significance of harm:

a) It is reasonably believed that the information has been or will be misused.
b) The unauthorized access, disclosure of loss was the result of malicious intent.
c) The Personal Information is sensitive.
d) Existing mitigating factors reduce the risk of Significant Harm.

“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 City.

“Use” means use of information by City employees for an authorized purpose that is authorized by directive or law.

Responsibilities

Head

The Head of the City is responsible for all obligations and discretionary decision-making under ATIA and POPA. The Chief Administrative Officer is the Head of the City.

Chief Legislative Officer (CLO)

The CLO performs the duties, powers and functions of the Head of the City for the purposes of the *Access to Information Act* and the *Protection of Privacy Act*.

Privacy and Access Coordinator (PAC)

The PAC is responsible for the overall management and coordination of privacy and access to information. The PAC is responsible for the following functions and activities:

PROGRAM MANAGEMENT

1. Ensuring that privacy, access and security program directives and procedures are developed, maintained, and updated, compliant with Access and Privacy Legislation.
2. Developing and completing quality assurance processes for implementation of the City’s privacy and information access management.
3. Providing training and resources as required in collaboration with the Human Resources department so that City employees, volunteers and contracted personnel are fully knowledgeable of their privacy and access duties, roles, responsibilities, and practices in compliance with the directive, procedures and Access and Privacy Legislation.
4. Representing the City in dealings with third parties, the provincial government, and the Office of the Privacy Commissioner of Alberta (OIPC), as necessary.

RIGHT OF ACCESS, CORRECTION AND COMPLAINTS

5. Responding to requests for access to information including, as necessary, assessment of fees, time extensions, disregarding requests, transfer of requests, duty to assist applicants, application of exceptions, Third Party Notifications, and public interest disclosure notice.
6. Responding to request for correction of Personal Information, including, as necessary, transfer of requests, correcting Personal Information, annotating Personal Information, notifying recipients.
7. Responding to requests for review of the handling of an access request or a privacy complaint including, as necessary, complaint submission, duty to assist the applicant, communicating with the OIPC, investigation, and responding to the applicant.

PRIVACY AND SECURITY OVERSIGHT

8. In consultation with City employees, providing advice, interpretation and implementation of applicable Access and Privacy Legislation regarding Personal Information, including release / non-release, collection, Use, and disclosure of Personal Information.
9. Maintaining the security, protection, and accuracy of Personal Information in the custody or control of the City in compliance with Access and Privacy Legislation, directives, and procedures.
10. Directing the response to privacy breaches of Personal Information in the City and its facilities in line with Access and Privacy Legislation and the Privacy Breach Response Procedures. (**Privacy, Access, and Security Governance Procedures Appendix 6)**
11. Completing Privacy Impact Assessments (PIAs) in collaboration with the department for project-specific Personal Information systems and practices.
12. Developing and maintaining a directory of Personal Information Banks and other registries required in collaboration with Records and Information Management (RIM) Services for identifying and tracking the collection, Use, disclosure, and security of Personal Information.

Chief Administrative Officer

The CAO is responsible for ensuring that privacy, access and security program directives and procedures in the City are aligned with governing mandates, standards, and planning.

Information Technology Management

IT Management, in coordination with the PAC as required, is responsible for all systems, networks and applications in alignment with this directive, Administrative Directives A-ITS-201 Information Security Management, A-ITS-101 Information Technology Authority and Responsibility and A-ITS-404 Access Management. IT is responsible for the following functions and activities:

1. implements and deploys privacy, access management, and security measures;

2. completes risk and mitigation assessments;
3. monitors and detects security threats;
4. assists in the response to Privacy Breaches.

Executive and Leadership Team

Executive Leadership and Leadership Team are responsible for implementing privacy and security directives and practices within their functional areas and are accountable for adherence to all directives by their employees and contracted third parties.

Leadership Team supports Executive Leadership to:

1. support their employees' awareness of and training on privacy and security directives and procedures;
2. implement privacy and security standards and processes in compliance with this directive and the procedures as they relate to information repositories and operational functions and activities of their area;
3. provide appropriate resources and facilities as needed to support the implementation of this directive and the procedures in their departments;
4. refer all formal right of access to information requests to the PAC;
5. cooperate and assist in locating and retrieving departmental information relevant to right of access requests;
6. report gaps in the privacy, access and security directive and procedures affecting their areas to the PAC; and
7. report any new information repositories or data systems that require registration, assessment, and information security classification to the PAC.

All City Employees and Service Providers

All City 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 shall:

1. make themselves aware of and adhere to this and all privacy, access and security program directives and procedures;
2. at the time of hire or engagement complete an oath of confidentiality;
3. capture, manage, access, release and protect information in their Custody or Control according to this and all privacy, access and security program directives and procedures and Access and Privacy legislation;
4. identify circumstances where a PIA may be required, including new or significantly changed programs, systems or administrative practices involving Personal Information, and notifying the PAC for guidance to initiate the process;
5. refer to the PAC all decisions about collection, Use, disclosure, and access that are not clearly directed by a directive or procedure;
6. report all suspected breaches to Personal Information to the PAC immediately upon discovery; and

7. identify and report information security incidents to the appropriate management according to privacy breach procedures **(Privacy, Access and Security Governance Procedures Appendix 6)**.

Expectations / Guidelines

Guiding Principles and Goals:

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

1. Program Accountability

   The City designates a position and individual who is accountable for implementing and maintaining access to information and privacy for information under the custody or control of the City.

2. Openness

   The City develops and follows access, privacy and security directives, procedures and practices that are compliant with Access and Privacy Legislation.

3. Collection of Personal Information

   The City 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.

4. Identifying Purposes

   When collecting Personal Information directly from an individual, the individual is informed of the purpose for which the information is collected.

5. 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.

6. Accuracy

   The City makes all reasonable efforts to ensure that both general information and Personal Information created or received by the City 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.

7. Right of Access

   Individuals have a right of access to all information, including Personal Information about themselves, that is in the City's custody or control, subject to limited and specific exceptions as set out in the Access and Privacy Legislation.

8. Safeguards

   The City 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.

9. Compliance Challenges

   Individuals are encouraged to bring any concerns or issues regarding privacy and access in the City to the Privacy and Access Coordinator for discussion and response. Individuals may appeal to the Information and Privacy Commissioner of Alberta to review or investigate the City's right of access or correction responses, or any directives or practices that they feel are not in compliance with legislative requirements.

Quality Assurance:

1. Directive Review

   The City reviews Privacy, Access, and Security directives to ensure that they are effective and align with legislative, regulatory or City functional developments and changes.

2. Training and Communication

   All City employees are provided with regular training resources to ensure they adequately understand and can implement all aspects of Privacy, Access, and Security.

   Training resources are reviewed to ensure that they are effective and align with legislative, regulatory or the City's functional developments and changes.

3. 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 City's information are identified, monitored, and assessed to determine the extent of the risk and the mitigation required.

   The City has audit logging, and monitoring of electronic systems that collect, Use, disclose or store Personal Information, data derived from Personal Information and Non-personal Data.

4. Privacy Impact Assessments

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.

The introduction of, or change to, a system, program, service, project, or practice is considered significant if:

a) the loss of, unauthorized access to or unauthorized disclosure of the Personal Information involved could result in Significant Harm;

b) it involves highly sensitive information;
c) it involves Personal Information of a significant percentage of the City's service population;
d) there is Data Matching of Personal Information with an external electronic information repository;
e) it is part of a common or integrated service or program;
f) the technology used is innovative; or
g) the administrative, technical, or physical measures and systems being proposed represent an additional risk to the privacy of individuals.

Any projects or changes of such nature are reported to the Privacy and Access Coordinator, who is responsible for ensuring the PIA is completed in conjunction with the relevant department who completes the initial draft of the PIA.

PIA content standards follow requirements set by the OIPC. The PIA is completed, submitted, and accepted by the OIPC before the project is implemented.

5. Personal Information banks

The City creates and maintains a directory of the Personal Information banks under its custody and control.

The City publishes the directory of its Personal Information banks, either in printed or electronic form, and makes it available to the public.

The Personal Information bank directory includes:

a) the title of the Personal Information bank;
b) the location of the Personal Information bank;
c) a description of the types of Personal Information included;
d) a description of the categories of individuals whose Personal Information is included;
e) the authority for collecting the Personal Information;
f) the purposes for which the Personal Information was collected or compiled; and,
g) the purposes for which the Personal Information may be Used or disclosed.

If Personal Information is Used or disclosed for a purpose other than the one described in the directory, the City

a) keeps a record of the purpose and connects that record to the Personal Information; and,
b) updates the directory to include the new purpose in the next publication of the directory.

Collection, Use and Disclosure of Personal Information

1. Collection of Personal Information

The City collects Personal Information only if:

a) the collection is expressly authorized by Access and Privacy Legislation;
b) the information is collected for the purposes of law enforcement; or
c) the information relates directly to and is necessary for an operating program or activity of the public body, including a common or integrated program.

The City collects Personal Information directly from the individual, or their authorized representative. The City only collects Personal Information indirectly from another source in the following circumstances:

a) the indirect collection is authorized by the individual, other legislation, or the OIPC;
b) the Personal Information may be disclosed to the City under the disclosure provisions outlined below;
c) the Personal Information is collected in a health and safety emergency, and the individual is unable to provide the information;
d) direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or of any other person;
e) the Personal Information is about a designated emergency contact;
f) the Personal Information is required to determine suitability for an honour or award;
g) the Personal Information is required to verify the individuals' eligibility for participation in a program or to receive a benefit, product, or service from the City;
h) the Personal Information is collected from public sources for fund-raising;
i) the Personal Information is required for a law enforcement purpose;
j) the Personal Information is required to collect a fine or debt owed to the public body, or for use in the provision of legal services to the City;
k) the Personal Information concerns the history, release, or supervision of an individual under the supervision of a correctional authority;
l) the Personal Information is required to inform the Public Trustee or Public Guardian about clients or potential clients;
m) the Personal Information is required for enforcing an order under the *Maintenance Enforcement Act*;
n) the Personal Information is required to manage or administer the City's personnel;
o) the Personal Information is required to support researching or validating claims, disputes, or grievances of aboriginal people;
p) the Personal Information is required to plan, manage, deliver, monitor, and evaluate a common or integrated program or service.

When collecting Personal Information directly from an individual, the City informs the individual of the purpose for which the information is collected, the legal authority for the collection, any intention to input the information into AI, and contact information of the individual who can answer questions about the collection.

Notifications are included on the medium or at the location of collection (websites, forms, pamphlets, posters). Notice is not required in circumstances when Personal Information is collected indirectly, for authorized purposes.

City employees collect only the amount and types of Personal Information as required to complete the stated function or purpose.

2. Consistent Purposes

The City will primarily Use and disclose Personal Information for the purpose for which it was originally collected or for a consistent purpose.

For a Use or disclosure to be for a consistent purpose, the City must determine that the proposed Use or disclosure is:

a) Directly connected to the original purpose for collection; and
b) Necessary for operating a program or common or integrated program or service of the City.

In assessing the consistent purpose, the City must consider:

a) The nature of the original purpose documented at the time of collection;
b) Whether the new Use or disclosure is a logical extension of that purpose;
c) The expected impact on the individual's privacy.

3. Use of Personal Information

The City may use Personal Information under the following circumstances:

a) for the purposes for which it was originally collected or for a use consistent with that purpose;
b) with the consent of the individual, when obtained in accordance with consent standards; or
c) for a purpose for which the information is disclosed to the City by another public body, under the allowable disclosure provisions.

City employees use only the amount and types of Personal Information as required to complete the state function or purpose.

4. Disclosure of Personal Information

The City may disclose Personal Information for the purpose for which the information was collected or compiled or for a purpose consistent with that purpose;

The City may disclose Personal Information for an inconsistent purpose only in the following circumstances:

INDIVIDUAL OR PUBLIC INTERESTS

a) with the consent of the individual, when obtained in accordance with consent standards;
b) to avert or minimize a risk of imminent harm and danger to the health and safety of any person;
c) so that the spouse or adult interdependent partner, relative or friend of an injured or deceased individual may be contacted, or to a relative of a deceased individual;
d) Personal Information of a minor or parent or guardian of a minor, to a law enforcement agency or to another organization or public body providing services to the minor, if it is clearly in the best interest of the minor;
e) to an MLA to assist the individual;
f) if disclosure is not an unreasonable invasion of privacy **(Privacy, Access, and Security Governance Procedures Appendix 4)**;

LEGAL OR ENFORCEMENT REQUIREMENTS

g) to comply with, or in accordance with, an enactment of Alberta or Canada;
h) in response to a subpoena, warrant, or court order;
i) for law enforcement purposes;
j) for the supervision of an individual by a correctional authority, or to a lawyer or student-at-law acting for an inmate;
k) to comply with the *Maintenance Enforcement Act*, or to the Administrator of the *Motor Vehicle Accident Claims Act*;
l) to an Officer of the Legislature if required for their duties;

OPERATIONAL REQUIREMENTS

m) to an officer or employee of the City if necessary for their duties;
n) to an officer or employee another public body if necessary for planning, managing, delivering, monitoring, or evaluating a common or integrated program or service;
o) to enforce a legal right, or to collect a fine or to make a payment, or for court and quasi-judicial proceedings;
p) to verify an individual's suitability or eligibility for a program or benefit;
q) to comply with the public interest disclosure provisions;
r) to the Auditor General or any other prescribed person for audit purposes;
s) to another public body for the authorized purposes of data matching;

HUMAN RESOURCES

t) to a union representative, with the consent of the individual;
u) for the management of personnel;

PUBLIC DISSEMINATION AND RESEARCH

v) to the Provincial Archives of Alberta or to City archives or another public body archives for archival preservation purposes;
w) for research or statistical purposes, under agreement;

x) when the information is available to the public.

City employees disclose only the amount and types of Personal Information as required to perform their assigned duties.

If there is no authority for the disclosure, the information cannot be disclosed. If The individual making the request for information wishes, they may make a formal ATIA Request.

The City will not sell Personal Information under its custody or control in any circumstance or for any purpose.

5. Research disclosure

Personal Information may be disclosed for statistical or research purposes, only if:

a) research cannot reasonably be accomplished in a non-identifiable form or is approved by the OIPC;
b) data matching resulting from the disclosure is not harmful to the individuals the information is about, and the benefits are clearly in the public interest;
c) The City has approved conditions relating to security and confidentiality, removal or destruction of individual identifiers, and prohibition of any subsequent Use or disclosure without authorization; and
d) all the conditions are set out in a written research proposal and agreement **(Privacy, Access, and Security Governance Procedures Appendices 2 and 3)**.

Data-Matching and Non-personal Data

The City

a) Data-matches Personal Information between two or more information sources to create new data derived from Personal Information; and
b) creates Non-personal Data from identifiable Personal Information;

only for the purposes of:

a) research and analysis; or
b) planning, managing, delivering, monitoring, or evaluating a program or service.

For the purposes of data matching, the City:

a) does not collect Personal Information directly from the individual;
b) may collect Personal Information from another public body;
c) may use Personal Information under its custody and control.

The City implements human oversight and validation measures for systems used for creating data derived from Personal Information or Non-personal Data to ensure the accuracy and reliability of the data.

The City retains and uses data derived from Personal Information only for the purpose for which it was created and as long is reasonably necessary to enable the City to carry out that purpose.

The City discloses data derived from Personal Information only

a) to the other public body from which data matched Personal Information was collected, for the purpose it was created;
b) to the Office of Statistics and information for the purposes of *The Office of Statistics and Information Act*.

The City uses Non-personal Data for any purpose and discloses Non-personal Data to anyone other than another public body only under agreement containing the required conditions, including prohibiting re-identification of individuals.

The City is not restricted from disclosing reports, summaries or other publications containing Non-personal Data that is aggregate or statistical form.

ARTIFICIAL INTELLIGENCE

1. Collection, Use and Disclosure

When the City makes use of AI, Personal Information is only collected, Used, and disclosed in compliance with Access and Privacy Legislation, this directive, and the City's AI Directive. All use of AI must follow A-ITS-406 AI Administrative Directive and AI Governance Procedures. The Personal Information activities may include:

INDIRECT COLLECTION

a) Accessing and compiling Personal Information from external networked sources or external datasets in response to prompts, either directly or through Large Language Models (LLMs).
b) Creation or generation of AI-Generated Content as a response to user prompts.

DIRECT COLLECTION

a) Collecting information from individuals in conversations or engagements through an AI chatbot service.

USE

a) Accessing and compiling Personal Information from internal sources and datasets in response to prompts, either directly or through LLMs.
b) Use of prompts, internal information and datasets, and generated inferences containing Personal Information to train internal LLMs.

DISCLOSURE

a) Disclosure of prompts and AI-Generated Content containing Personal Information to external parties.
b) The City considers information about individuals extracted by AI from external networked sources, including the internet, as Personal Information.
c) The City only uses AI that does not disclose internally generated Personal Information in prompts or internal information sources to an external LLM for AI training purposes.

2. Notification

The City notifies individuals that AI has and is being used to:

a) Collect Personal Information in conversations or direct engagements with individuals; or
b) Generate information or knowledge that contributes to decision-making about the individual.

All new high-risk AI activities require a Privacy Impact Assessment before they are initiated.

Right of Access and Correction

1. Receiving and facilitating requests

Requests for access to City information can be made by any individual or organization (the applicant), regardless of location or status. A public body may not make a request to another public body.

The City responds to right of access requests openly, accurately, and completely and will:

a) engage with applicants to allow them to clarify their request so it can be processed;
b) respond to questions in plain language, and
c) assist applicants in adjusting requests so they can be processed.

The City does not deny access to information based on the applicant's reason or purpose for the request.

Requests for information under ATIA may contain Personal Information of the applicant, which will be protected and managed in accordance with POPA.

Once the applicant has met the requirements to make a request, the City has thirty business days to respond, unless the request has been abandoned, disregarded or transferred, or if the time limit is extended in accordance with ATIA.

2. Excluded records

Some records that are in the custody or control of the City are excluded from the ATIA and do not have to be considered relevant or released as part of a right of access request. However, the City may choose to release this information as part of a request under specified circumstances. Excluded records include:

a) Records designated by the City as available without a request;
b) Court and administrative support records created or received by the courts of Alberta, including justices of the peace;
c) Records created or received by officers of the Alberta Legislature, including the OIPC, Ethics Commissioner, Auditor General, and the Public Interest Commissioner;
d) Records and copies of records from a provincial or public body registry office, including the Personal Property Registry, Corporate Registry, Motor Vehicles Registry, Land Titles Office, and the Vital Statistics Registry;
e) City records that have already been made public by other means;

f) Records in the custody or control of the federal, provincial, or territorial government and their agencies;
g) Personal or constituency records of an elected or appointed member of the governing body of the City;
h) A question used on an examination or test only if release does not jeopardize a standardized or continuing evaluative process.

These excluded records can only be used or disclosed with the consent or permission of the individual or organization:

a) Records from private sector donors that are preserved in City archives for historical research purposes.

Data derived from Personal Information and Non-personal Data cannot be released in response to a right of access request.

3. Disregarding requests

The City disregards a right of access request only in exceptional circumstances when:

a) the information requested is already available to the applicant or to the public;
b) after initial requests from the City for clarification, the applicant has not provided enough detail to make it comprehensible or to locate the requested information;
c) the request has been made repeatedly, as part of a pattern of conduct that is systematic, regular, and deliberate;
d) the applicant makes use of abusive, threatening, or harassing language or actions during the application or facilitation process; or
e) the request is abusive, threatening, frivolous or vexatious.

The applicant is informed of the reasons for disregarding the request and the right to ask the Commissioner to review the City's decision.

4. Searches for relevant records

The City makes every effort to identify and retrieve for review all records in its Custody or Control that are relevant to an applicant's request. This will include information in any location and format and on any devices, accounts and platforms not owned by the City, which was created or received by employees and contractors to support their functions as City officials.

The search for records relevant to an applicant's request includes all electronic records that can be accessed or produced using normal computer hardware, software and technical expertise and would not unreasonably interfere with its operations. This includes:

a) reports or extracted data sets from existing databases that can be constructed and generated using existing software and expertise, but does not include the creation of information that is an analog summary, analysis, consolidation, or digest of existing information that did not exist prior to the request;

b) emails, text messages, and social media posts sent or received on any account or platform that were created or received to support functions and activities of the public body.

City Privacy and Access officials responsible for responding to a request are authorized to access and retrieve for review any personal or general information on any device or platform that is required to identify, retrieve records relevant to a request.

5. Reviewing and withholding information

The City only withholds information relevant to the request when it is determined that mandatory or discretionary exceptions to the right of access apply to the records requested.

The City must refuse to disclose information in response to a right of access request if the release would be:

a) harmful to business interests of a third-party business;
b) an unreasonable invasion of a Third Party's personal privacy; or
c) harmful to provincial Cabinet and Treasury Board confidences, as long as the information is in a record for less than 15 years or result in the release of a record that was submitted to or prepared for submission to the Executive Council, the Treasury Board or one of their committees, or was created on or on behalf of any of the above.

The City may refuse to disclose information in response to a right of access request if the disclosure could reasonably be expected to:

a) threaten anyone's safety or mental or physical health; interfere with public safety; or cause an applicant to do immediate and grave harm to themselves or others;
b) reveal confidential evaluations conducted pre-hire or pre-contract award;
c) harm a law enforcement matter;
d) harm a workplace investigation;
e) harm inter-governmental relations;
f) reveal local public body confidences, including drafts of bylaws, resolutions, legal instruments, and the substance of deliberations of in-camera meetings;
g) reveal advice, proposals, recommendation, analyses, or process options developed by or for the public body;
h) cause harm to the economic interests of the City or the Alberta Government;
i) reveal information relating to testing or auditing procedures;
j) reveal legally privileged information;
k) cause harm to conservation of heritage sites; or
l) reveal information that is already or will be made available to the public within sixty business days.

6. Public health and safety override

The City discloses to the public, a group of people, an individual, or an applicant, any information that the City has about a risk of Significant Harm to the

environment or to the health and safety of the public, a group of people, an individual or an applicant.

Before disclosing the information, the City must, where practicable, notify any Third Party to whom the information relates, give the Third Party an opportunity to make representations relating to the disclosure and notify the Commissioner.

7. Third Party reviews

The City notifies and requests advice from affected third parties when it is unclear whether the relevant records hold information that, if released, would be:

a) harmful to business interests of a third-party business;
b) an unreasonable invasion of a Third Party's personal privacy.

8. Requests for correction or amendment of Personal Information

Individuals may request correction or amendment of their own Personal Information in the Custody or Control of the City.

The City will not amend professional opinions that are made by employees that have the competency to make them.

Privacy Breach Response

Privacy Breach response steps can be found in the **Privacy, Access and Security Governance Procedures Appendix 6 and the Response Form Appendix 7.**

1. Determining level of response

The severity of the Privacy Breach determines the nature of the response reporting structure, remedial action, and the investigation process. In the response process, severity is based on:

a) The security classification of the information, which considers potential and real harm to individuals and organizations;
b) The internal and external scope and scale of the Privacy Breach;
c) The known relationship of the recipients to subject individuals; or
d) The intentionality of the cause.

Levels are determined when any of the designated classes and circumstances apply as indicated in the Privacy Breach Response Procedure, Step 1 Identifying and Reporting the Privacy Breach which incorporates an assessment of the real risk of Significant Harm because of a Privacy Breach.

2. Investigation principles

The City uses generally accepted investigative methods to obtain the most effective results while respecting the rights, privacy, and dignity of persons being investigated. Investigations will, as required, incorporate the following methodologies:

a) Keep investigation information confidential to protect the privacy of individuals investigated and to maintain the integrity of the investigation;
b) Use surveillance or monitoring data to establish past or current actions on an as-needed basis;

c) Examine or confirm the veracity of facts or statements, sometimes using Third Party witnesses;
d) Inform participants of their status and the progress of the investigation as fully and quickly as possible so long as it does not jeopardize the integrity of the investigation;
e) Base findings and conclusions on balance of probabilities.

The Privacy Breach investigation is an administrative process rather than a disciplinary process. Once the report is delivered, it is the responsibility of Management, Executive Leadership, and the Director most responsible for Human Resources to determine the appropriate disciplinary action, if any.

Complaint Resolution

1. Submission

Members of the public may submit a complaint in writing to the City for investigation and resolution. Verbal complaints will not be treated as formal complaint submissions by the City.

Complaints may concern any decision, act, or failure to act by the City in a formal access to information request or in the protection of Personal Information, data derived from Personal Information, and Non-personal Data under the City's custody or control or by a City employee, including:

a) a contravention in the creation, collection, Use, or disclosure of Personal Information, data derived from Personal Information, or Non-personal Data;
b) a refusal, without justification, to a correction of Personal Information;
c) the actual or attempted re-identification, by any person, of Non-personal Data;
d) failure by a City employee to provide a duty to assist;
e) a contravention in the application of a time extension in a formal access request;
f) the inappropriate levy of a fee applied in a formal access request.

Complaints related to unauthorized disclosure, Use, destruction, loss, removal, or modification of Personal Information will initiate the Privacy Breach response process, which may proceed in conjunction with the complaint process.

2. Principles of Investigation and Response

The Privacy and Access Officer receive, processes, investigates, and responds to complaints under ATIA and POPA made to the City.

If an investigation is required to establish findings for a complaint, the City uses generally accepted investigative methods to obtain the most effective results while respecting the rights, privacy, and dignity of the complainant and any employees involved. Complaint investigations will, as required, incorporate the following methodologies:

a) Keep investigation information confidential to protect the privacy of the complainant and any individuals investigated and to maintain the integrity of the investigation;

b) Use surveillance or monitoring data to establish past or current actions on an as-needed basis;
c) Examine or confirm the veracity of facts or statements, sometimes using Third Party witnesses;
d) Base findings and conclusions on balance of probabilities.

Records created, collected, or processed as part of a complaint investigation are classified according to the Information Security Classification system and will not be provided as part of the complaint response. Requests by the complainant for investigation records associated to the complaint will be treated as a formal access to information request, and records will be managed according to that process.

The complaint investigation is an administrative process rather than a disciplinary process. Once the report is delivered, it is the responsibility of Management Executive Leadership and the director most responsible for Human Resources to determine the appropriate disciplinary action, if any.

RESPONSE

The City acknowledges, in writing, receipt of the complaint. All acknowledgements of submission will include:

a) reference to the initial complaint;
b) an internal assigned file number; and
c) the estimated date of response, within thirty business days of the date the complaint was received.

The City provides responses in writing, containing the findings of the Privacy and Access Officer, to all formal complaint submissions.

Response time is dependent on the need for an investigation and the complexity of the associated investigation.

The complaint response will include the following:

a) the internal assigned file number;
b) a copy of the original complaint submission and a list of any records the complainant submitted with the complaint;
c) the findings of the Privacy and Access Officer and the reason for the findings or a statement of justification; and
d) contact information for the Office of the Information and Privacy Commissioner and directions for submitting a request for review to the Commissioner.

Legal References
Access to Information Act, SA 2024, c A-1.4, as amended
Protection of Privacy Act, SA 2024, c P-28.5, as amended
Records Bylaw, 2/2006, as amended

Cross References
A-LS-03 - RIM Program Directive and Records Classification and Retention Schedule
A-LS-05 - Digitization of Records

A-LS-13 Electronic Signatures Directive
A-HRS-02.05 - Corrective Actions Directive
A-HRS-02.04 – Code of Conduct
A-ITS-101 - Information Technology Authority and Responsibility
A-ITS-201 - Information Security Management
A-ITS-205 - Server and Network Physical Security (Confidential under Section 21 of ATIA, Section 10 of POPA)
A-ITS-404 - Access Management
A-ITS-406 - Acceptable Use of Artificial Intelligence Directive
Cyber Security Event Management Plan (**Confidential** under *Section 21 of ATIA, Section 10 of POPA*)

Procedures

The procedures for this Directive are contained within the Privacy, Access and Security Governance Procedures and will be updated as required in conjunction with current Access and Privacy Legislation and changes within the City's business requirements.

CHIEF ADMINISTRATIVE OFFICER SIGNATURE	CHIEF ADMINISTRATIVE OFFICER APPROVAL DATE
William Fletcher (Jun 8, 2026 15:49:14 MDT)	06/08/2026

DATE REVIEWED	NEXT REVIEW DATE	DATES OF REVISIONS
June 8, 2026 - LLRS	**June, 2027 – LLRS**	**N/A**

A-LS-07 Privacy, Access and Security Administrative Directive

Final Audit Report 2026-06-08

Created:	2026-06-08
By:	Janice Vollrath (jvollrath@stalbert.ca)
Status:	Signed
Transaction ID:	CBJCHBCAABAAXO89rk_16x7-TV5JQaDi8EPxRT7k_Qdq

"A-LS-07 Privacy, Access and Security Administrative Directive" History

Document created by Janice Vollrath (jvollrath@stalbert.ca)
2026-06-08 - 7:37:49 PM GMT- IP address: 205.206.72.240

Document emailed to wfletcher@stalbert.ca for signature
2026-06-08 - 7:38:44 PM GMT

Email viewed by wfletcher@stalbert.ca
2026-06-08 - 9:48:46 PM GMT- IP address: 104.47.75.190

Signer wfletcher@stalbert.ca entered name at signing as William Fletcher
2026-06-08 - 9:49:12 PM GMT- IP address: 96.52.57.1

Document e-signed by William Fletcher (wfletcher@stalbert.ca)
Signature Date: 2026-06-08 - 9:49:14 PM GMT - Time Source: server- IP address: 96.52.57.1 - Signature Appearance Selected: DRAW

Agreement completed.
2026-06-08 - 9:49:14 PM GMT