Purpose

1. The purpose of this Policy is to identify the City's Privacy Management Program and to provide direction and guidance to Employees regarding adherence to and compliance with Privacy Legislation.

POLICY STATEMENTS

2. The following statements provide guidance and direction for the City's management of information:

(a) **Openness and Transparency -** The City develops and follows access, privacy and security policies and practices that are compliant with Privacy Legislation. Such policies and practices are publicly available.

(b) **Designation of Privacy Officer -** The City designates a position of Privacy Officer that is accountable for implementing and maintaining access to information and privacy of information under the custody or control of the City.

(c) **Collection of Personal Information -** The City collects personal information only for authorized purposes and only to the extent that it relates directly to and is necessary for an operating program or activity of the City. When collecting personal information directly from an individual, the City informs the individual as required by the *Protection of Privacy Act* related to the collection.

(d) **Use and Disclosure of Personal Information -** The City only uses and discloses personal information 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 individual.

(e) **Correction of Personal Information -** The City makes all reasonable efforts to ensure that both general information and personal information created or received by the City are 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.

(f) **Information 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. In the event of a privacy incident, the City will respond in a timely manner and as required by the *Protection of Privacy Act*.

(g) **Compliance Challenges and Privacy Complaints -** The City encourages individuals to bring forward to the City any concerns or issues regarding access and privacy at the City. The City acknowledges that in certain situations individuals may appeal to the Privacy Commissioner of Alberta to review or investigate the City's right of access or correction responses, or any policies or practices that they feel are not in compliance with legislative requirements.

(h) **Right of Access -** The City respects the right of access of individuals to all information, including personal information about themselves, that is under the custody or control of the City, subject to limited and specific exceptions.

Privacy Management Program

3. The City is committed to protecting personal information and to transparency in governance and strives to comply with and fulfill its duties under Privacy Legislation.

4. The City has implemented a Privacy Management Program that consists of this Policy, as well as the other City governance documents identified in this Policy. Together, these documented policies and procedures promote the City's adherence to and compliance with Privacy Legislation.

5. The City's Privacy Management Program is applicable to:

   (a) all Employees;

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

   (c) all facilities and equipment required to collect, manipulate, transport, transmit, or keep City information.

6. The governance documents that comprise the City's Privacy Management Program, including this Policy, will be reviewed, assessed, and updated at least every three years.

GUIDELINES

Openness and Transparency

7. Except for certain technical information, security-related information, and other information that could compromise the security of personal information in the custody or under the control of the City, the City makes its Privacy Management Program publicly available on the City's website.

Designation of Privacy Officer

8. The Privacy Officer for the City for the purposes of POPA is the individual in the Access & Privacy Analyst position. If that position is vacant, then the Privacy Officer is the individual in the Corporate Risk Management Section Manager position.

Collection of Personal Information

9. The City only collects personal information as allowed by POPA and the Access & Privacy Procedure and Access to Information & Protection of Privacy Corporate Procedure 7016.01-CP. The City will only collect personal information if:

   (a) the collection is authorized by 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 City, including a common or integrated program of service.

10. The City collects personal information directly from an individual and informs the individual of the information required by Section 4 of POPA.

11. The City only collects personal information indirectly (from another source) in those circumstances authorized by Section 5 of POPA. In both circumstances, the City collects only the amount and types of personal information as is necessary to fulfill the purpose for such collection.

Use and Disclosure of Personal Information

12. The City may only use and disclose personal information in accordance with Privacy Legislation and the Access to Information & Protection of Privacy Corporate Procedure 7016.01-CP.

13. The City may use and disclose personal information:

    (a) for the purposes for which it was collected or compiled or for a use consistent with that purpose;

    (b) with the consent (whether oral, electronic, or written) of the individual, when that consent is obtained in accordance with Privacy Legislation and the Access to Information & Protection of Privacy Corporate Procedure 7016.01-CP; or

    (c) for a purpose for which the information may otherwise be used or disclosed pursuant to Privacy Legislation.

14. The City will not sell personal information in its custody or under its control in any circumstances or for any purposes, including for marketing or advertising purposes.

Correction of Personal Information

15. If an individual believes there is an error or omission in basic information about themselves (such as a change of name or address), then they may contact the department identified in the notification of collection or privacy statement for that collection to request that such information be corrected or amended.

16. If an individual believes there is an error or omission in the individual's personal information that is other than basic information, then they may make a formal request to correct or amend information to the Privacy Officer.

17. The department or the Privacy Officer, as applicable, will receive, process, and respond to such request in accordance with POPA, the Access & Privacy Procedure, and the Access to Information & Protection of Privacy Corporate Procedure 7016.01-CP. Despite the foregoing and pursuant to POPA, the City will not correct an opinion, including a professional or expert opinion.

Information Security

Data Matching, Data Derived from Personal Information & Non-Personal Data Management

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

(a) the City may only carry out data matching to create data derived from personal information for one or more of the following purposes:
  (i) research and analysis;
  (ii) planning, administering, delivering, managing, monitoring, or evaluating a program or service; or
  (iii) one or more purposes prescribed in Privacy Legislation;

(b) for the purposes of data matching, the City:
  (i) does not collect personal information directly from an individual;
  (ii) collects personal information from another public body;
  (iii) may use personal information in its custody or under its control; and

(c) the City discloses data derived from personal information only to:
  (i) the other public body from which data matched personal information was collected, for the purpose it was created;
  (ii) the Office of Statistics and Information for the purposes of the *Office of Statistics and Information Act*.

19. Until the applicable governance document is in effect, the Director of Information Management must be consulted before carrying out data matching.

Artificial Intelligence and Automated Systems

20. When the City uses personal information in an automated system to generate content or make decisions, recommendations, or predictions, the City 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 of Information Management must be consulted before such use is made.

Privacy, Access, and Security Monitoring and Assessment

21. The City proactively monitors and assesses its systems, circumstances, practices, and repositories to identify risks or gaps in standards relating to the privacy, accessibility, usability, integrity, retention, continuity, and security of personal information to determine the extent of the risk and the mitigation required. Making the details of these monitoring practices public could compromise the security of the personal information, and so that information will be withheld and not made publicly available on the City's website.

Information Safeguards

22. The City complies with the POPA requirement to protect personal information in its custody or under its control by adhering to reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal, or destruction. Such arrangements are set out in the Records Retention & Disposition Bylaw 3305/2003, Information Management Policy 5207-CA, Records Management Policy 5210-CA, Records Management Procedure 5007-CP, and the Retention, Disposition and File Classification Manual, and includes administrative, technical, and physical safeguards for managing personal information, data derived from personal information, and non-personal data. 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 City's website.

Information Security Classification

23. The City has established and adheres to a security classification system for personal information, data derived from personal information, and non-personal data in its custody or under its control. Such security classification system and related information is set out in the Records Retention and Disposition Bylaw 3305/2003, Information Management Policy 5207-CA, Records Management Policy 5210-CA, Records Management Procedure 5007-CP, and the Retention, Disposition and File Classification Manual.

Compliance Challenges and Privacy Complaints

24. If a person believes that their personal information has been collected, used, or disclosed by the City in contravention of POPA, then they may submit a complaint to the Privacy Officer. The Privacy Officer will receive, process, and respond to such complaint in accordance with Privacy Legislation.

25. If a person has a concern or issue regarding access and privacy at the City, they may submit their concern or issue to the Privacy Officer. The Privacy Officer will receive, review, and respond to such concern or issue in accordance with Privacy Legislation.

Right of Access

26. If a person desires access to records in the custody or under the control of the City, or an individual desires access to personal information about themselves that is held by the City, then they may submit an access to information request to the City. The Employee with delegated authority to do so (which may be the Privacy Officer or another Employee) will receive, process, and respond to that request in accordance with ATIA.

Privacy Incidents

27. 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 City, then the Employee will immediately notify the Privacy Officer and adhere to the Privacy Breach Protocol Corporate Procedure 7016.02-CP.

28. Upon notification from an Employee, or the Privacy Officer otherwise becoming aware of the occurrence of such an incident, the Privacy Officer will give notice, without unreasonable delay, of the incident in accordance with Privacy Legislation.

Privacy Impact Assessments

29. The City will complete privacy impact assessments for any new, or a substantial change to an existing, administrative practice, program, project, or service that will involve the collection, use, or disclosure of personal information when required under POPA, including when one or more of the following apply:

    (a) the loss of, unauthorized access to, or unauthorized disclosure of the personal information could result in significant harm; or

    (b) a practice, program, project, service or system will collect, use, or disclose personal information deemed to be of high sensitivity;
        (i) will involve the personal information of a significant percentage of the population the City serves;

(ii) will involve data matching between two or more public bodies;
(iii) is part of a common or integrated program or service; or
(iv) involved the development or use of innovative technology.

30. The department pursuing a system, project, program, service, or practice of such nature will report their intent to the Privacy Officer. Thereafter, the department and the Privacy Officer will collaborate to complete the privacy impact assessment in accordance with POPA. If required by POPA, the Privacy Officer will submit the completed document to the Information and Privacy Commissioner of Alberta.

Mandatory Training

31. All Employees must complete the training required by the Privacy Officer about the obligations of those Employees under Privacy Legislation.

32. New Employees will be required to complete the training within thirty days of commencement of employment, unless they are a returning Employee whose training has not expired in accordance with the below.

33. Refresher training is required every three years for supervisors and managers, and every five years for all other Employees.

34. Upon completion of training or retraining, all Employees must email a copy of their certificates to corporatetraining@reddeer.ca.

35. Employees must maintain valid training during the performance of any service for the City.

Privacy Management Plan

36. In addition to this Policy, the City's Policy Management Plan includes:

Access to Information & Protection of Privacy – Delegation Policy 7016-CA
Information Technology Use and Security Policy 5201-CA
Medical Records Information Procedure 2007-CP
Identity Verification Procedure 5209-CP
Information Technology Security Incident Plan Procedure 5203-CP

ROLES, RESPONSIBILITIES & ACCOUNTABILITIES

City Manager

37. The City Manager is designated as the head of the City for the purposes of Privacy Legislation pursuant to the City Manager & Designated Officers Bylaw 3685/2022, and may delegate to any person any power, duty, or function of the head under Privacy Legislation, except the power to delegate.

38. The City Manager is responsible for ensuring the City's compliance with Privacy Legislation. Unless otherwise delegated, the City Manager is responsible for all obligations and discretionary decision-making under Privacy Legislation.

Director of Corporate Risk Management

39. The Director of Corporate Risk Management is responsible for:

(a) overseeing and supporting the Privacy Officer and the Privacy Management Program;

(b) overseeing the review of the Access & Privacy Policy, and overseeing the development and implementation of the Access & Privacy Procedure; and

(c) assisting the Privacy Officer in response to privacy incidents, as needed.

Director of Information Management

40. The Director of Information Management is responsible for:

(a) implementing and deploying privacy and security measures;

(b) completing risk and mitigation assessments;

(c) monitoring and detecting security threats;

(d) managing the City's fulfillment and adherence to those guidelines set out above under the 'Information Security' heading of this Policy for all systems, networks, and applications; and

(e) assisting the Privacy Officer in response to privacy incidents, as needed.

Senior Management & Section Managers

41. Senior Management and Section Managers are responsible for:

(a) implementing and adhering to the information access, privacy, security, and retention policies and practices as set out in the Privacy Management Program within their divisions and departments;

(b) supporting their Employees' awareness of and training on information governance and access and privacy;

(c) referring, and ensuring their Employees refer, all access to information requests made under ATIA to the Privacy Officer;

(d) reporting any new information repositories or data systems that require registration, assessment, and security classification to the Privacy Officer and Director of Information Management;

(e) reporting gaps in privacy, access and security policies affecting their areas to the Privacy Officer; and

(f) cooperating and assisting, and ensuring their Employees cooperate and assist, in locating and retrieving departmental information relevant to access to information requests made under ATIA and as requested by the Privacy Officer.

Employees

42. Each Employee is responsible for:

(a) at the time of hire, signing a confidentiality agreement;

(b) making themselves aware and taking the mandatory training on information governance, information security, and access and privacy;

(c) implementing privacy and security for all information they create and receive as part of their functions and activities;

(d) adhering to the information access, privacy, security, and retention policies and practices as set out in the Privacy Management Program;

(e) report all suspected breaches to personal information to the Privacy Officer immediately upon discovery; and

(f) identify and report information security incidents to the appropriate management according to privacy breach procedures.

DEFINITIONS

In this Policy, the following words and phrases have the following meanings:

"**ATIA**" means the *Access to Information Act*, SA 2024, c A-1.4;

"**Employee**" means City employees, and any person who performs a service for the City as an appointee, volunteer, student, or under a contract or agency relationship with the City;

"**POPA**" means the *Protection of Privacy Act*, SA 2024, c P-28.5;

"**Privacy Legislation**" means collectively: ATIA; Access to Information Act Regulation, Alta Reg 133/2025; POPA; Protection of Privacy (Ministerial) Regulation, Alta Reg 143/2025; and Protection of Privacy Regulation, Alta Reg 132/2025; and

"**Privacy Management Program**" means the City's documented policies and procedures that promote its compliance with its duties under Privacy Legislation, as more specifically described in this Policy under the heading 'Privacy Management Plan'.

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

References to statutes and bylaws in this Policy are references to the statutes or bylaws including any amendments and replacement statutes and bylaws, and regulations and orders under them.

REFERENCES/LINKS

Access to Information Act

Protection of Privacy Act

Inquiries/Contact Person:

1 City Manager
2 Privacy Officer

Document History:

Date:	Approved/Reviewed By:	Title:
June 11, 2026	"Tara Lodewyk"	City Manager