Statement of Policy and Procedure			
Department:	City Manager	Policy No.	**115**
Section:	City Clerk	Issued:	January 23, 2023
Subject:	**Privacy and Confidentiality Policy**	Effective:	January 23, 2023
Council Resolution # and Date:	Council Resolution No. 0017 dated January 23, 2023		
		Replaces:	
Issued by:	Wenda Atkinson, Corporate information Manager	Dated:	
Approved by:	Terri Mercier, City Clerk		

1 POLICY

1.01 The City of Prince Albert (The City) is responsible for transparency and good stewardship of all confidential information in its possession or control. As such the protection of all personal, third party and confidential city business information is managed in accordance with *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP).

1.02 The City of Prince Albert is committed to protecting the privacy of all individuals who entrust their personal information with The City, in accordance with the standards set out in LAFOIP.

2 PURPOSE

2.01 The purpose of this policy is to guide and inform City of Prince Albert employees, council members and contracted third parties of their responsibilities to ensure all personal information, third party and confidential city business information is managed and protected during its collection, use, disclosure, storage, and destruction life cycle in accordance with LAFOIP and *The Cities Act.*

3 SCOPE

3.01 This policy applies to members of City Council, City employees, and contracted third parties who collect, use, disclose, store and destroy personal information, third party information and confidential city business information on behalf of The City.

4 RESPONSIBILITIES

4.01 All Employees and members of City Council

a. Be familiar with and abide by this policy.

b. Are responsible for protecting personal information, third party information and confidential city business information obtained or accessed during the course of their work on behalf of The City.

c. Are responsible for proactively incorporating privacy protection into all corporate initiatives.

d. Are responsible to report all breaches of this policy to the City Clerk's Office.

4.02 Directors/Managers/Supervisors

a. Ensure employees are provided the opportunity to attend training related to privacy and confidentiality.

b. Cooperate with and assist the City Clerk's Office during privacy breach reviews and fill out appropriate forms.

4.03 Contracted Third Parties

a. Be familiar with and abide by this policy.

b. Are responsible for protecting personal, third party and confidential city business information obtained or accessed during the course of their work on behalf of the City.

c. Are responsible to report all breaches of this policy to the City Clerk's Office.

4.04 Information Technology

a. Assist in identifying risks that may impact privacy and security and facilitate reasonable mitigation measures.

b. Assist with privacy breach risk mitigation measures involving technology.

4.05 **City Clerk**

a. Provide guidance and decision making on privacy and confidentiality matters.

b. Coordinate and oversee all actions in response to an alleged privacy breach.

c. Provide training and education opportunities regarding privacy and confidentiality.

d. Provide recommendations regarding privacy risk mitigation.

5 DEFINITIONS

5.01 **Administrative Safeguards** include policies, procedures, agreements, contracts, and training resources to protect the personal information of individuals, as well as third party and other confidential City information.

5.02 **Authorized Employees** means only those approved employees who have the authority to provide the required services or action for a specific function.

5.03 **Collection** means the act of gathering, acquiring, recording, or obtaining personal or confidential information from any source and by any means.

5.04 **Confidential City Business Information:** is information exempt from disclosure in LAFOIP including but is not limited to:

a. Solicitor/Client Privilege;

b. Information if released could harm the economic/financial and other interests of the City;

c. Labour/Personnel Matters;

d. Negotiations;

e. Information from other governments;

f. Proposed policies or draft bylaws or resolutions and matters that have not been discussed or released publicly.

5.05 **Consent:**

Before personal information (PI) is utilized for any other purpose than identified at the time of collection, The City must obtain written or express consent from the individual before their personal information can be utilized for any other purpose.

Implied Consent arises when consent may reasonably be inferred from the action or inaction of an individual and that an individual has a certain understanding, knowledge, or acceptance, of when their consent might be implied.

Opt-in Consent occurs when an individual is given an opportunity for an individual to express positive agreement to the stated purpose or the individual takes action to be included to the purpose.

Opt-out Consent occurs when an individual is given the opportunity to express non-agreement to an identified purpose. An individual takes the action to "opt out" of the purpose or say "no". The individual should be clearly informed that the failure to advise will mean that the individual is consenting to the proposed use or disclosure of the specified information.

5.06 **Contracted Third Party** means an individual or company hired to work on behalf of The City.

5.07 **Disclosure** of information is the sharing of personal information with a separate entity or organization, not a department, division or section of the City.

5.08 **Employees** means City employees, including volunteers, individuals under contract to perform City business, and appointed members of a City Committee, Board or Commission.

5.09 **Need to know** means accessing and restricting the collection and disclosure of information to only what information is required to perform a task or provide a service.

5.10 **Personal Information** means information about an identifiable individual including but is not limited to information about an individual's: race; religion; family status; age; birthdate; place of origin; employment or criminal history; financial information; health services number; driver's license number; social insurance number; home address or telephone number. Personal Information may also include the views or opinions of someone about that person or information about the physical or mental condition.

5.11 **Physical Safeguards** include locked filing cabinets, restricted access to areas containing personal, third party or other confidential information and, computer monitor privacy screens and alarm systems.

5.12 **Privacy** is the protection and security of personal, confidential, sensitive, and third party information.

5.13 **Privacy Breach** occurs when there has been unauthorized access to or disclosure of personal or confidential information; or a secondary use of personal information not consistent with the original purpose.

5.14 **Record** means information in any form and includes information that is written, photographed, recorded, digitized or stored in any manner, but does not include computer programs or other mechanisms that produce records.

5.15 **Technical Safeguards** include the use of strong passwords, encryption, automatic logoff features for computers, and firewalls to protect sensitive electronic personal, third party or other confidential information.

5.16 **Third Party Information** means trade secrets of a third party; financial, commercial, scientific, technical or labour relations information that is supplied in implicit or explicit confidence to the City by a third party.

5.17 **Use** of information is the internal use of the information by the City and includes sharing within the City, when necessary, in a way that remains under the control of the City.

6. PRINCIPLES:

6.01 **Accountability:** The City is responsible for personal and confidential information under its control. The City has designated the City Clerk to be accountable for compliance with the following principles.

6.02 **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the City at or before the time the information is collected.

6.03 **Consent:** Implied or expressed consent is required for the collection, use, or disclosure of personal information, subject to the exceptions contained in LAFOIP. Consent should be given voluntarily and be fully informed when possible. The individual can also revoke their consent.

6.04 **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purpose for which it is being collected.

6.05 **Limiting the use, disclosure, and retention of personal information:** personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary to meet the original purposes, or as permitted by the City's Retention Bylaw, as amended from time to time.

6.06 **Accuracy:** Personal Information shall be as accurate, complete and up-to-date as is necessary for the purposes it is to be used.

6.07 **Safeguards:** Personal and confidential information shall be protected by reasonable safeguards against risks such as loss, theft, and unauthorized access.

Safeguards refer to a combination of policies, procedures, practices and technologies regardless of form in which the information is stored (e.g. paper, electronic).

6.08 **Openness:** The City shall make its policies and practices relating to the management of personal and confidential information readily available.

6.09 **Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of their personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

6.10 **Challenging Compliance:** An individual shall be able to address concerns related to compliance with any of the above principles to the City Clerk Office. If the individual remains dissatisfied with the City's response, the individual has a right to address their concerns with the Information Privacy Commissioner of Saskatchewan (IPC).

7. STATEMENTS OF POLICY

7.01 All employees are responsible for protecting personal information and the City's business information obtained or accessed during the course of their work within the City.

7.02 All obligations to protect personal, third parties and the City's business information continue indefinitely, even after discontinuation of employment/association/ privileges with the City.

7.03 The collection, use, or disclosure of personal, third parties and the City's business information is acceptable only on a need to know basis for the provision or support of legitimate duties for the City.

7.04 In all cases of collection, use or disclosure, the personal, third parties and the City's business information that is collected, used or disclosed should be limited to the least amount of information required to serve the purpose.

7.05 Secondary use (use of information for other than the original purpose) without the individual's consent must be:

a. In accordance with LAFOIP or *The Cities Act*; and
b. Approved through the Privacy Impact Assessment tool process.

7.06 The City shall protect personal Information, third party information and confidential third party information by making reasonable security arrangements. The security arrangements will include a system of administrative, physical and technical controls, including but is 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 general public; and
c. Securing the rooms and filing cabinets that contain Personal Information during those times in which an authorized person is not present.

7.07 All members of Council, employees or contracted third parties **shall not** use their position with the City in order to collect or access personal, third parties and the City's business information that is not required for employment related purposes.

7.08 All members of Council, employees or contracted third parties are required to review this policy and seek answers regarding the policy prior to or at the commencement of their employment/privileges/association with the City.

7.09 All City employees review the Conflict of Interest Policies as required by *The Cities Act.*

7.10 At the direction from the City Clerk, Information Technology will conduct audits of electronic applications for compliance with this policy.

7.11 Records shall only be destroyed in a confidential manner in accordance with the City's Record Retention Bylaw.

7.12 Privacy impact assessment tools are required when a new project, program, activity or substantial change to an existing program is being initially considered. The tools will assist the City to identify the risks to confidential information, assist the project team to mitigate the risks building privacy into the process design.

8. **NON-COMPLIANCE** with this policy may result in disciplinary action up to and including termination of employment.

A privacy breach may be reported to the IPC. The IPC may recommend the Ministry of Justice charge an individual with an offence under LAFOIP. Any person who knowingly contravenes LAFOIP may be subject to a fine of not more than $50,000 and/or not more than one (1) year of imprisonment.

9. REFERENCES & RELATED FORMS

The Local Authority Freedom of Information and Protection of Privacy Act
The Cities Act
The Local Authority Freedom of Information and Protection of Privacy Regulations
The Cities Regulation
Record Retention Bylaw

Access to Information Policy
Conflict of Interest Policy
Utilization of Electronic Devices with Monitoring Capabilities Policy
Gift, Favours and Entertainment Policy
Employment of Relatives Policy
Occupational Health & Safety Policy – Harassment Safety Administrative Policy
Progressive Discipline Policy
Social Media, Media Relations and Public Statements Policy

Privacy Impact Assessment
Preliminary Privacy Impact Assessment

10. PROCEDURES

10.01 PRIVACY IMPACT ASSESSMENTS

10.01.1 A privacy impact assessment is required when personal information, third party information or other confidential City business information is involved; and

a. A new project, program, activity or system is being initially considered;

b. A significant change is being made to an existing program;

c. A previous privacy impact assessment has not been done, or

d. There are changes to the way the information is being handled.

10.01.2 The City Clerk's Office leads the privacy impact assessment process.

10.01.3 The preliminary privacy impact assessment tool (Pre PIA) is completed by the Department Project Lead as a step in the project or change as a privacy risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology, program, or process or other activity may have

on personal, third party or other confidential City business information. The Pre PIA will help to determine whether a full privacy impact assessment is required.

10.01.4 The Pre PIA is signed by the project lead, Director of IT, IT Lead, Department Director, City Clerk's Office and the City Manager.

10.01.5 The City Clerk's Office determines whether a full privacy impact assessment is to be completed.

10.01.6 If a full privacy impact assessment is not required, in that there are no privacy or confidentiality impacts or issues identified by the City Clerk's Office, the review is complete and the Pre PIA is appropriately filed as a record.

10.01.7 If a full privacy impact assessment is required, in that privacy and confidentiality impacts have been identified, details are documented on the form which include the following information:

a. type and sensitivity of personal, third party and other confidential City business information involved.

b. identification of how the information is being collected, created, used, disclosed, stored, transmitted, retained and disposed of.

c. what administrative, technical and physical safeguards are in place to protect this information from unauthorized access, use and disclosure.

d. how the project's business processes will relate to other existing or planned programs, systems or processes, including how information flows from one to another, and

e. what further information technology and security considerations are needed.

10.01.8 The City Clerk's Office identifies privacy risks and impacts and recommends measures to mitigate these risks. The full privacy impact assessment is signed by the Department Project Lead, Department Director, Information Technology Manager where the project or initiatives involves technology solutions, the City Clerk's Office and the City Manager. Any privacy mitigation measures with financial implications require review by the Director of Financial Services and City Manager.

10.01.9 The City Manager is responsible for decisions made regarding the recommendations put forward by the City Clerk's Office.

10.02 **PRIVACY BREACH**

10.02.1 In the event of a breach of personal, third party or other confidential City business information, the following is required immediately:

a. Stop the practice and recover and/or secure the affected records.

b. Notify the applicable Department Director and City Clerk.

10.02.2 Following containment of the breach, the breach is investigated and documented, including:

a. Details of the privacy breach and factors contributing to the breach,

b. Evaluation of immediate and ongoing privacy risks, identification of safeguards in place prior to the incident

c. Whether applicable procedures were followed, and,

d. Determination of whether any changes to procedures, policies, or safeguards are required.

10.02.3 The City Clerk will determine whether the situation requires further notification to internal employees or City Council, the IPC, affected individuals or law enforcement.

10.02.4 In the event that the IPC launches an investigation, a report will be submitted to the Commissioner by the City Clerk's Office.