CITY OF PRINCE GEORGE
ADMINISTRATIVE PROCEDURE

PROCEDURE NAME: **Privacy Management Program**

CATEGORY:	Government – Effective Governance
APPROVED BY CITY MANAGER (Version 1):	2019/06/03
APPROVED BY CITY MANAGER (Version 2):	2023/03/27
DEPARTMENT RESPONSIBLE:	Office of the City Manager – Legislative Services Division

PURPOSE:

This Privacy Management Program Administrative Procedure (the "Privacy Management Program Procedure") provides a framework and expectations for the Privacy Management Program for the City of Prince George (the "City"). It seeks to ensure that Personal Information is responsibly managed in accordance with the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

This Procedure seeks to support the privacy of individuals' whose personal information is collected, used and disclosed by the City by clearly articulating roles and responsibility for privacy management within the City.

Key components of the City's Privacy Management Program include:

- accountability for privacy management requirements, including the designation of a privacy officer for the City;
- development, completion and review of corporate privacy policies that ensure lawful collection, use, disclosure, storage, retention and disposal of Personal Information;
- development, completion and review of Privacy Impact Assessments;
- development, completion and review of Information Sharing Agreements, and other agreements as outlined in FIPPA;
- management of the Personal Information Inventory;
- management of Privacy Breach incidents and complaints;
- development, completion, review and implementation of compliance and auditing tools and processes;
- ensuring that contracted service providers are aware of and accountable for their privacy obligations to the City;
- on-going employee privacy awareness and education;
- routine review, auditing and assessment of this Privacy Management Program.

MSWord Document Number: 664934
PDF Document Number: 665139

SCOPE:

This Privacy Management Program Procedure applies to all City Employees.

DEFINITIONS:

The following definitions are provided for key terms and acronyms used in this Privacy Management Program Procedure:

"Common or Integrated Program or Activity" means a program or activity that provides one or more services through (i) one or more other public bodies or agencies working collaboratively, or (ii) one public body working on behalf of one or more other public bodies or agencies, (iii) is confirmed by regulations under FIPPA as being a common or integrated program or activity; and (iv) is confirmed by a written agreement that complies with regulations under FIPPA.

"Contact Information" means information to enable an individual at a place of business to be contacted, including the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

"Employee" means a person who is employed by the City or a volunteer and includes a service provider.

"Department Head" means a Director of a City administration department.

"FIPPA" means the *Freedom of Information and Protection of Privacy Act,* R.S.B.C., 1996, c. 165, and regulations thereto, as amended from time to time.

"FIPPA Coordinator" is the designated privacy officer for the City, and the person(s) designated as a "Coordinator" under the City of Prince George Freedom of Information and Protection of Privacy Bylaw No. 8689, 2015, as amended from time to time.

"FIPPA Head" means the person designated as the "Head" under the City of Prince George Freedom of Information and Protection of Privacy Bylaw No. 8689, 2015, as amended from time to time.

"Information Sharing Agreement" means an agreement between the City and another person, organization or entity that provides for the sharing or exchange of Personal Information and sets conditions on the collection, use or disclosure of Personal Information by the parties to the agreement.

"Personal Information" means recorded information about an identifiable individual other than Contact Information.

"Personal Information Bank" means a collection of personal information that is organized or retrievable by the name of an individual or by identifying number, symbol or other particular assigned to an individual.

"Personal Information Inventory" means an inventory listing the categories, locations, purposes, authority and sensitivity of the City's Personal Information holdings.

"Privacy Management Program Procedure" means this Privacy Management Program Administrative Procedure of the City, as amended from time to time.

"Privacy Breach" means access to, or collection, use, disclosure or disposal of Personal Information, whether accidental or deliberate, that is not authorized under FIPPA.

"Privacy Impact Assessment" or "PIA" means a process that is conducted by the City to determine if a current or proposed or significantly revised enactment, system, project, program or activity meets or will meet the requirements of FIPPA.

"Privacy Protection Schedule" means a schedule of terms and conditions approved by the FIPPA Coordinator and applicable to the collection, use, disclosure, retention, protection and processing of Personal Information by vendors or service providers engaged by the City.

"Record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic or otherwise, but does not include a computer program or any other mechanism that produces records.

"Service Provider" means a person, including a corporation or society, retained under contract to perform services for the City.

"**Significant Harm**" means identity theft or significant bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, negative impact on a credit record or damage of or loss of property.

PROCEDURE:

1. PRIVACY MANAGEMENT PROGRAM PROCEDURE STATEMENT

1.1 This Privacy Management Program Procedure is established in accordance with the City of Prince George Freedom of Information and Protection of Privacy Bylaw No. 8689, 2015 and section 36.2 of FIPPA.

1.2 The City protects the Personal Information it collects, uses, and discloses in accordance with FIPPA, by promoting privacy awareness, application of sound privacy principles, and implementation of reasonable security measures to protect Personal Information.

1.3 This Privacy Management Program Procedure is the foundation for the City's Privacy Management Program and sets the framework for privacy to be a central component of the City's business practices and a built-in component of day-to-day program operations.

2. AUTHORITY

2.1 The FIPPA Head is responsible for managing and overseeing the implementation of and compliance with this Privacy Management Program Procedure.

3. ROLES & RESPONSIBILITIES

3.1 City Manager

The City Manager shall be responsible for:

- ensuring all Employees are given notice of and access to a copy of the most recent version of this Privacy Management Program Procedure; and
- ensuring the roles and responsibilities listed under section 3.2 below that are in the "City Manager's Office" administrative department are fulfilled.

3.2 Department Heads

Each Department Head shall, within their Department, be responsible for:

- ensuring Employees are familiar with and comply with their obligations under this Privacy Management Program procedure and FIPPA;
- creating and maintaining an awareness among Employees of privacy protection and the responsible collection, use, disclosure, storage, retention and disposal of Personal Information;
- cooperating with and supporting the FIPPA Head in carrying out their duties and responsibilities, including under this Privacy Management Program Procedure;
- assigning resources to support compliance with this Privacy Management Program Procedure and FIPPA;
- ensuring Privacy Impact Assessments are completed as required by this Privacy Management Program Procedure, and implementing all actions required by a Privacy Impact Assessment applicable to their department;
- ensuring Information Sharing Agreements are completed as required by this Privacy Management Program Procedure, and implementing all actions required by an Information Sharing Agreement applicable to their department.
- providing requested assistance to the Privacy Coordinator and FIPPA Head in ensuring that the Personal Information Inventory remains current.

3.3 FIPPA Head

The FIPPA Head has the following roles and responsibilities:

- approving amendments to this Privacy Management Program Procedure as may be necessary or desired, in consultation with the City Manager;
- coordinating the implementation of this Privacy Management Program Procedure;

- liaising with the Office of the Information and Privacy Commissioner ("OIPC"), including in relation to investigations;
- reviewing and commenting and providing required approvals on Privacy Impact Assessments, Information Sharing Agreements and other privacy-related agreements;
- ensuring the Personal Information Inventory is maintained and kept current;
- ensuring Employees have access to training and education relating to the City's duties under FIPPA, including regarding the collection, use, disclosure, storage, retention and disposal of Personal Information; and
- carrying out the duties and responsibilities of the "Head" as set out in FIPPA.

3.4 FIPPA Coordinator

The FIPPA Coordinator has the following roles and responsibilities:

- supporting and assisting the FIPPA Head in their roles and responsibilities;
- receiving, reviewing and responding to access requests made under Part 2 of FIPPA,
- remaining current and knowledgeable about the types of Records made routinely available within departments, and remaining aware of circumstances that may require an applicant to file a formal request under FIPPA;
- remaining current and knowledgeable of the City's Personal Information holdings;
- advocating for protection of Personal Information in dealings with City departments;
- consulting with and providing recommendations to the FIPPA Head in relation to the City's compliance with FIPPA.

3.5 All Employees

All Employees have the following roles and responsibilities:

- complying with this Privacy Management Program Procedure and other City privacy-related policies, guidelines and directions;
- completing training on FIPPA, including regarding the collection, use, disclosure, storage, retention and disposal of Personal Information, as appropriate to their work function;
- conducting Privacy Impact Assessments and Information Sharing Agreements in the manner and form directed by the FIPPA Head, and keeping the FIPPA Head informed of changes to initiatives that require updates to a Privacy Impact Assessment or Information Sharing Agreement;

- supporting the FIPPA Head in creating and ensuring that the Personal Information Inventory and Personal Information Bank applicable to their work function is accurate and complete;
- immediately reporting an actual or reasonably suspected Privacy Breach as set out in this Privacy Management Program Procedure;
- reporting privacy complaints as set out in this Privacy Management Program Procedure;
- including the Privacy Protection Schedule or privacy protection language, as deemed appropriate by the FIPPA Head or FIPPA Coordinator, in all contracts with Service Providers that involve collection, use or disclosure of Personal Information;
- referring requests for access to or correction of Personal Information to the FIPPA Coordinator; and
- cooperating with the FIPPA Head and FIPPA Coordinator in implementing this Privacy Management Program Procedure and in complying with FIPPA.

4. EDUCATION AND AWARENESS

All Employees shall participate in privacy training opportunities made available by the City, including:

4.1 For all Employees: training on FIPPA and privacy generally as appropriate to their work function;

4.2 For Employees handling high-risk or sensitive Personal Information electronically, in coordination with the IT Services Department's training, training related to information systems and their security;

4.3 For Employees managing programs or activities, training related to Privacy Impact Assessments; and

4.4 For Employees managing a Common or Integrated Programs or Activity, training related to Information Sharing Agreements.

5. PRIVACY IMPACT ASSESSMENT or PIA

5.1 All Employees shall provide their full cooperation to ensure that Privacy Impact Assessments are performed in relation to all new and significantly revised Initiatives;

5.2 Department Heads shall be responsible for conducting Privacy Impact Assessments for Initiatives within their Department in accordance with the City's PIA template. and any related Procedures.

5.3 Department Heads will ensure Privacy Impact Assessments are prepared, completed and submitted to the FIPPA Head for review, comment and approval at the earliest practicable opportunity during the development of any proposed enactment, system, project, program, or activity (an "initiative") involving Personal Information, and for any significant modifications to existing initiatives involving Personal Information.

5.4 Department Heads are responsible for ensuring that they do not engage in any Initiative involving the storage of or disclosure of personal information outside of Canada unless they have first completed a PIA in accordance with the requirements of FIPPA, and that PIA has been approved by the FIPPA Head.

5.5 The FIPPA Head will ensure that each approved PIA is retained in the Legislative Services division.

6. INFORMATION SHARING AGREEMENTS

6.1 Any necessary Information Sharing Agreements are to be completed by the applicable Department Head or designated program area employee with guidance from the FIPPA Head.

6.2 The applicable Department Head will ensure implementation of all actions required by an Information Sharing Agreement.

7. PERSONAL INFORMATION INVENTORY and PERSONAL INFORMATION BANK

7.1 The City will maintain a Personal Information Inventory that will involve collaboration with all City administrative departments.

7.2 The FIPPA Coordinator will update the Personal Information Inventory with Personal Information Banks and Information Sharing Agreements that result from new initiatives involving Personal Information identified in a Privacy Impact Assessment.

8. PRIVACY BREACH MANAGEMENT

8.1 An Employee must immediately report an actual or reasonably suspected Privacy Breach to their Department Head in accordance with the City's Privacy Breach Procedure.

8.2 The Department Head must immediately report a Privacy Breach to the FIPPA Head and collaborate with the FIPPA Head through the response protocol in accordance with the City's Privacy Breach Procedure.

8.3 The FIPPA Head is responsible for the investigation and risk management of a Privacy Breach as set out in the City's Privacy Breach Procedure.

8.4 As described in the City's Privacy Breach Procedure, the City follows the following steps in responding to a Privacy Breach.

Step 1 Containment of the breach, recovery of confidential or Personal Information and reporting the incident;

Step 2 Investigation and evaluation of the risks of the unauthorized disclosure of Personal Information;

Step 3 Notification of individual(s) affected as determined necessary; and

Step 4 Prevention strategies to safeguard against future breach incidents.

The steps may occur concurrently, in quick succession, or in a different order. The first three steps must be undertaken as soon as possible following the Privacy Breach. The fourth step involves investigation into the cause of the Privacy Breach and may require a security audit of both physical and technical security.

8.5 The FIPPA Head, or their delegate, is responsible for making required reports of Privacy Beaches to the Office of the Information and Privacy Commissioner and affected individuals in circumstances where the Privacy Breach may be expected to result in Significant Harm to the individual.

9. ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

9.1 Employees receiving a formal request under FIPPA for access to or correction of an individual's Personal Information in the custody or control of the City are to promptly forward the request to the FIPPA Coordinator for response.

9.2 Employees receiving a routine request from an individual to correct their factual Personal Information, such as a change or update to a residential or other personal mailing address, personal e-mail address or personal phone number, may make the requested change without forwarding the request to the FIPPA Coordinator.

10. PRIVACY RELATED COMPLAINTS

10.1 An Employee receiving a complaint related to the City's collection, use or disclosure of Personal Information is to promptly refer the complainant to the FIPPA Head or the FIPPA Coordinator for response.

10.2 The City will receive and respond to privacy complaints it receives, including by conducting investigations where appropriate.

11. ACCURACY OF PERSONAL INFORMATION

11.1 The City will make reasonable efforts to ensure that the Personal Information it relies on to make a decision directly affecting an individual is accurate and complete.

12. DEMANDS FOR DISCLOSURE

12.1 An Employee who receives a demand from a third party for disclosure of Records or Personal Information must immediately notify the FIPPA Head, including any warrant, order, subpoena or any demand or applications materials made in connection with legal proceedings.

13. SERVICE PROVIDER MANAGEMENT

13.1 Employees who prepare or manage contracts are to include a Privacy Protection Schedule in all contracts that involve the Service Provider having access to, or collecting, using or disclosing, Personal Information in the custody or under the control of the City.

14. COMPLIANCE REVIEWS AND AUDITS

14.1 The FIPPA Head may conduct compliance reviews and audits in order to assess compliance with FIPPA and this Privacy Management Program Procedure and will communicate the results to the City Manager and the Department Heads.

14.2 The City Manager and the FIPPA Head shall conduct routine reviews of the City's Privacy Management Program and this Procedure to ensure it remains current and effective.

15. PROTECTION OF PERSONAL INFORMATION

15.1 The City and all Employees must comply with the obligation under FIPPA to protect Personal Information within the City's custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.