PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

PURPOSE

To establish guidelines for the collection, use, disclosure, storage, and retention of personal information by the City of Fort St. John (the "**City**") and to ensure personal information in the custody or under the control of the City is protected.

To ensure the City, as a public body, manages personal information in accordance with the *Freedom of Information and Protection of Privacy Act,* RSBC 1996, c 165 ("***FIPPA***").

SCOPE

This Policy applies to all employees, elected officials, and volunteers of the City. The privacy obligations of the City equally apply and flow down to all service providers where collection, use, disclosure, security, and access to personal information may be required while performing services under contract to the City.

FIPPA and the regulations under it prevail over this policy.

POLICY STATEMENT

The City is subject to *FIPPA* and is committed to the responsible management of personal and confidential information within the City's custody and control.

This Policy is established in accordance with the City's Freedom of Information Bylaw, the "**FOI Bylaw**".

INTERPRETATION

In this Policy:

> **"contact information"** is 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 e-mail, or business fax number of the individual.

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

"day" does not include Saturday, Sunday or holidays.

"employee" means a person who is employed by the City, an elected official of the City, or a volunteer of the City.

"Head" means the person designated in the FOI Bylaw as the City's head for the purposes of *FIPPA.*

"Information and Privacy Coordinator" means the person(s) designated in the FOI Bylaw to be responsible for assisting the Head in administering the City's responsibilities under *FIPPA,* as delegated by the Head.

"Information Sharing Agreement" or **"ISA"** means an agreement between the City and:

(a) another public body under *FIPPA*;
(b) a government institution subject to the *Privacy Act* (Canada);
(c) an organization subject to the *Personal Information Protection Act* (British Columbia) or the *Personal Information Protection and Electronics Documents Act* (Canada);
(d) a public body, government institution, or institution as defined in applicable provincial legislation having the same effect as *FIPPA*;
(e) a person or group of persons; or
(f) an entity prescribed in the *FIPPA* regulation,

that 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.

"Privacy Impact Assessment" means an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program, or activity meets or will meet the requirements of Part 3 of *FIPPA.*

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

"Privacy Program Manual" means the established procedures to ensure the responsible management of information within the City's custody and control.

"service provider" means a person retained under contract to perform services for the City.

AUTHORITIES

1. The City's Corporate Officer is the Head and:

   (a) is responsible for the development, maintenance, and oversight of the Privacy Program for the City, which establishes the necessary policies and procedures to ensure the responsible management of information within the City's custody and control;
   (b) has the authority and responsibility to manage and implement this Policy;
   (c) is the City's designated liaison with the Office of the Information and Privacy Commissioner (OIPC) on all matters related to information access and privacy under *FIPPA*; and
   (d) may delegate any of the Head's duties under *FIPPA*.

2. The City's Deputy Corporate Officer is an Information and Privacy Coordinator and will assist the Head with their duties, and when delegated by the Head, will have the authority to perform all of the Head's duties.

3. The Administrative Assistants I and II in Legislative Services, and the Records Management Coordinator are Information and Privacy Coordinators and will provide administrative support to the Head and the Deputy Corporate Officer, as directed.

COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION

Collection

4. The City will only collect personal information, directly or indirectly, per Part 3 of *FIPPA*, including, without limitation, in the following circumstances:

(a) where collection of information is authorized under a statute;
(b) for the purposes of City services, programs, and activities;
(c) for the purposes of planning or evaluating City services, programs, and activities;
(d) for law enforcement purposes, including the enforcement of City bylaws; or
(e) by observation at presentations, ceremonies, performances, sports events, or similar events, that are open to the public and where the person voluntarily appears.

5. The City will only collect personal information directly from the individual the information is about, unless it is through a method authorized under Part 3 of *FIPPA*.

6. When personal information is collected directly from an individual, and not otherwise exempted in section 27(3) of *FIPPA*, the City will ensure that any individual from whom the City collects personal information is first provided with the:

(a) the purpose for collecting it;
(b) the legal authority under which it is collected; and
(c) provide contact information for a City employee who can answer questions about the collection.

Use

7. The City will only use the personal information in its custody or under its control:

(a) for a purpose for which that information was obtained or compiled, or for a use consistent with that purpose (i.e. where the use has a reasonable and direct connection to the original purpose, or is otherwise necessary to comply with the City's statutory duties, or to run a program or activity of the City);
(b) with prior written consent of the individual whom the information is about (consent should specify how and to whom the information will be used or disclosed); or
(c) for a purpose for which that information may be disclosed under sections 33 to 34 of *FIPPA.*

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

Disclosure

8. All employees, including service providers and their employees or associates, who have access (authorized or unauthorized) to personal information in the custody or under the control of the City, will not disclose that information except in accordance with *FIPPA*.

9. The City will only disclose personal information in its custody or under its control as permitted by *FIPPA,* including, without limitation, in the following circumstances:

   (a) if the person has identified the personal information to be disclosed and consented in writing to its disclosure;
   (b) in accordance with an enactment of British Columbia or Canada that authorizes or requires its disclosure;
   (c) to employees if the information is necessary for their duties, for delivery of a common or integrated program or activity, or for planning or evaluating a City program or activity;
   (d) if the personal information is made publicly available in British Columbia by a provincial law that authorizes or requires that it be made publicly available;
   (e) to a public body or law enforcement agency to assist in a specific investigation or law enforcement proceeding; or
   (f) to the City's legal counsel for the purpose of legal advice or for use in legal proceedings involving the City.

10. When the City obtains an individual's written consent to disclose or release personal information, the employee obtaining that consent will take reasonable steps to verify that individual's identity.

Accuracy

11. The City will make reasonable efforts to ensure that personal information which is relied upon to make decisions directly affecting an individual is accurate and complete.

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

Access

12. Anyone may ask for a copy of their personal information that is in the custody or under the control of the City by writing to the Head. Please note the following:

(a) If a person is an employee and would like a copy of their employee personal information, that person must make that request through the City's Human Resources department.
(b) A person requesting a copy of their personal information must verify their identity, to the satisfaction of the City, before the requested personal information is disclosed by the City. Government-issued photo identification is the preferred method of verification. Where a person does not have government-issued photo identification, the request will be referred to the Head who will determine the appropriate method of identification.

Correction

13. If a person believes there is an error or omission in their personal information which is in the custody or under the control of the City, that person may, by writing to the Head, request that their personal information be corrected.

14. The City will, within 30 business days of receiving a request for the correction of personal information, either:

(a) correct the personal information as requested, or
(b) if a decision is made not to correct the information as requested, annotate the personal information with the requested correction and notify the requester with reasons if the decision is made to not correct the information as requested.

15. Upon correcting or annotating personal information, the City will notify any other public body or third party to whom that information has been disclosed during the one (1) year period before the correction was requested.

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

16. On being notified of a correction or annotation of personal information made by another public body, the City will make that correction or annotation on any record of that personal information in its custody or under its control.

VIDEO SURVEILLANCE

17. The City will follow Video Surveillance Guidelines and Procedure for the collection, security, retention, use, disclosure, and disposal of video surveillance footage captured on and around the City's municipal properties.

RETENTION AND DISPOSAL

18. The City will, at a minimum, keep all records in the custody and under the control of the City, for one (1) year from the date it is collected, except where an earlier disposal date is set out in the City's records retention policy.

19. If an individual's personal information, which is in the custody or under the control of the City, is used by or on behalf of the City to make a decision which directly affects that individual, the City will ensure that this personal information is retained for at least one (1) year after it is used.

INFORMATION SECURITY

20. The City will protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or disposal of personal information, considering the sensitivity of the information, the likelihood of damage occurring, and the potential harm which could be caused if there were a breach.

21. All employees are required to respect the confidentiality of personal information they receive or compile and are required to collect, use, and disclose personal information only in accordance with this Policy and *FIPPA.*

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

22. When travelling with personal information or working offsite at another location, employees and service providers must take measures to protect electronic and paper records containing personal information.

23. Before discussing personal information with an individual, employee, third party, or authorized representative, employees must verify the individual's identity and, where appropriate, their authority to act on behalf of an individual.

24. Employees and service providers (where the service provider is accessing personal information while performing their duties under contract to the City) must complete a privacy training session provided by the City and the training process will be documented. The training will be assessed and revised to ensure the knowledge on privacy processes and practices is current.

25. Employees must use their City assigned corporate email account when conducting any City business. Whenever possible employees should not send personal information via email, and personal identifiers should never be used in the subject of an email. If email must be used to send personal information, ensure that the documents containing personal information are password protected. Do not send the password by email but instead provide it by telephone or other means.

26. If personal information is disclosed to a service provider, the City will impose contractual protections on the service provider. Those protections will vary according to the nature and sensitivity of the personal information involved and will be outlined in their contract's Privacy Protection Schedule.

PRIVACY COMPLAINTS

27. Individuals have the right under *FIPPA* to file a complaint about the improper collection, use, or disclosure of their personal information by the City, or about a decision made by the City concerning a personal information request. Privacy complaints that are received by the City must be referred to the Head who will investigate the complaint and remediate as required.

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

PRIVACY BREACH PROCEDURE

28. A privacy breach occurs when personal information is accessed, collected, used, disclosed, or disposed of in a way that does not comply with the provisions of *FIPPA*.

29. All employees have a duty under section 30.5 of *FIPPA* to immediately report suspected privacy breaches to the Head.

30. When a privacy breach is suspected or has occurred, the Head, or their delegate, will then take the following steps:

(a) Containment:

(i) If possible, promptly contain the breach by suspending or causing to be suspended the process or activity that caused or contributed to the breach; and
(ii) Take steps to recover the confidential or personal information, if possible (see sections 73.1 and 73.2 of *FIPPA*).

(b) Investigation, Evaluation, and Notification:

(i) Initiate an investigation and evaluate risks associated with the breach;
(ii) From the results of the initial investigation, determine if:
  (A) the breach should be reported to the Privacy Commissioner;
  (B) notification of affected persons is required and, if so, notify those affected persons;
  (C) notification of law enforcement, insurers, service providers, regulatory bodies, is required, and, if so, notify those organizations or entities;
  (D) further investigation into the cause and extent of the breach is necessary;
(iii) Ensure the details of the breach and corrective actions are documented; and

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

(iv) If the investigation was initiated by way of complaint, respond to the complainant in writing to provide the result of the investigation.

(c) Prevention:

(i) Review investigative findings and develop strategies to prevent similar privacy breaches from occurring in the future; and
(ii) Implement prevention strategies and monitor them through privacy audits at least annually.

31. If a breach has occurred, or is suspected to have occurred, an affected individual will be notified of the breach by the Head if such a notification is necessary to avoid or mitigate harm that will result from the unauthorized collection, use or disclosure of personal information.

32. If the breach is widespread or the City does not have the contact information for an affected individual, the Head may choose to notify affected individuals indirectly (ie. social media, website, press release, etc.).

33. All employees will cooperate and promptly assist the Head, or their delegate, with any investigation into a privacy breach.

COMPLAINTS

34. Any complaints regarding the City's compliance with *FIPPA*, or any inquiry concerning the City's privacy policy or practices should be in writing and sent to the Head.

35. Employees receiving a complaint related to the City's collection, use, or disclosure of personal information are to promptly refer the complainant to the Head for a response. There are tight timelines under *FIPPA* for such requests, so prompt forwarding is vital.

36. Upon receiving a complaint, the City will send a written acknowledgement to the complainant within 14 business days.

37. The City will follow the Privacy Breach procedures, set out in this Policy, and the Privacy Management Manual when responding to complaints of a privacy breach.

38. Within 30 business days of receiving a complaint, the City will respond to the complainant in writing to provide the result of the investigation of the complaint, subject to operational requirements and timelines.

PRIVACY IMPACT ASSESSMENT

39. Before developing a program, system, or any other initiative that involves the collection, use, or disclosure of personal information, the City will complete a Privacy Impact Assessment, which will include a description of measures to mitigate any identified privacy risks.

40. In the Privacy Impact Assessment, the City will identify the authority for the collection, use and disclosure of personal information under *FIPPA.*

AUDIT AND EVALUATION

41. The Head will audit the City's information handling and privacy management program at least annually.

42. The Head will prepare a report to the Executive Leadership Team documenting findings in detail and advising of any concerns.

EDUCATION AND AWARENESS

43. Privacy training for employees should be provided upon hire with refresher training provided annually thereafter. Training is required as set out below:

    (a) For all employees: training on *FIPPA* and privacy generally as determined to be appropriate in consideration of the employee's roles and responsibilities.

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

(b) For employees handling high-risk or sensitive personal information electronically: training related to information systems and their security.
(c) For employees managing programs or activities: training related to Privacy Impact Assessments.
(d) For employees managing a common or integrated program or activity: training related to Information Sharing Agreements.

INFORMATION SHARING AGREEMENTS (ISA)

44. If the City is sharing personal information with an organization, public body, or agency external to the City, the employee responsible for that program or activity should, where applicable, complete an ISA in accordance with the ISA Guidelines set in the Privacy Program Manual, and any further directions provided by the Head.

45. An ISA is considered to be completed once it has been fully signed by all of the required parties.

46. Any employee completing an ISA will ensure that the Head is consulted throughout the process and promptly provided with a copy of the completed ISA.

47. The City will comply with all lawful terms and conditions of an ISA to which it is a party.

CONTACT INFORMATION

For questions about this policy or about personal information, please contact:

Corporate Officer
City Hall - 10631 – 100 Street
Fort St. John, BC V1J 3Z5
(250) 787-8150

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/24

If a person needs information or advice, they can also contact the OIPC. A person may also file a complaint directly with the OIPC, but are encouraged to follow the City's complaint process initially, to work towards a satisfactory resolution of the complaint directly.

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038 Stn. Prov. Govt.
Victoria B.C. V8W 9A4

(250) 387-5629

info@oipc.bc.ca