PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

PURPOSE

A. 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.

B. 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.

FIPPA and the regulations under it prevail over this Policy.

POLICY STATEMENT

This Policy is established in accordance with the City's Freedom of Information Bylaw, No. 2426, 2018 (the "**FOI Bylaw**").

INTERPRETATION

In this Policy:

"day" does not include Saturday, Sundays 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 Coordinators" 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.

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

INTERPRETATION

In this Policy:

"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, which 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 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.*

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

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

AUTHORITIES

1. The City's Director of Legislative and Administrative Services is the Head and:

   (a) has the authority and responsibility to manage and implement this Policy,
   (b) is the City's designated liaison with the Office of the Privacy Commissioner on all matters related to information access and privacy under *FIPPA*, and
   (c) may delegate any of the Head's duties under *FIPPA*.

2. The City's Deputy City Clerk 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 any or all of the Heads duties.

3. The City's Administrative Assistants I and II are Information and Privacy Coordinators, and will provide administrative support to the Head and the Deputy City Clerk, as directed by the Head or Deputy City Clerk.

COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

Collection

4. The City will only collect personal information, directly or indirectly, in accordance with 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 evaluation 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.

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

Collection (continued)

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* (see section 27).

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 (ie. 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 36 of *FIPPA.*

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

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. 140/19

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 will be 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).

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

Correction (continued)

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.

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.

RETENTION AND DISPOSAL

17. 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.

18. 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

19. 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, taking into account the sensitivity of the information, the likelihood of damage occurring, and the potential harm which could be caused if there were a breach.

20. 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. 140/19

INFORMATION SECURITY (continued)

21. If personal information is disclosed to a service provider, the City will make reasonable efforts to impose contractual protections on the service provider. Those protections will vary according to the nature and sensitivity of the personal information involved.

22. All personal information collected by the City will be stored within Canada or in accordance with section 30.1 of *FIPPA.*

PRIVACY BREACH PROCEDURE

23. A privacy breach occurs when personal information is accessed, collected, used, disclosed or disposed of without proper authorization.

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

25. 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;

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

PRIVACY BREACH PROCEDURE (continued)

25. **(b) Investigation, Evaluation, and Notification:** (continued)

(ii) From the results of the initial investigation, determine if: (continued)
(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
(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 finding 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.

26. 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 which will result from the unauthorized collection, use or disclosure of personal information.

27. 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.).

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

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

COMPLAINTS

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

30. 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.

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

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

33. 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

34. 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.

35. 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

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

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

AUDIT AND EVALUATION (continued)

37. The Head will prepare a report to the General Manager of Corporate Services documenting his or her findings in detail and advising of any concerns.

EDUCATION AND AWARENESS

38. Privacy training for employees 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.
(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)

39. 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 out in Schedule A to this Policy, and any further directions provided by the Head.

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

41. 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.

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

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

CONTACT INFORMATION

The Head:

Director of Legislative and Administrative Services
City Hall - 10631 – 100 Street
Fort St. John, BC V1J 3Z5
(250) 787-8150

If a person has any questions about this policy or their personal information, they may contact:

Director of Legislative and Administrative Services or Deputy City Clerk
City Hall - 10631 – 100 Street
Fort St. John, BC V1J 3Z5
(250) 787-8150

If a person needs information or advice, they can also contact the Office of the Information and Privacy Commissioner for British Columbia (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.

The Office of the Information and Privacy Commissioner can be reached as follows:

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

Location
4th Floor, 947 Fort Street, Victoria BC V8V 3K3

Telephone
(250) 387-5629

Email
info@oipc.bc.ca

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

SCHEDULE A

INFORMATION SHARING AGREEMENT GUIDELINES

An ISA is a formal agreement that describes the terms and conditions for sharing personal information.

An ISA should, depending on the circumstances, be prepared any time the City plans to share personal information with an organization external to the City. Whether an ISA is required will be determined by the volume, degree of access, and sensitivity of the personal information being shared. The Head should be consulted if there is any doubt.

An ISA may impose additional obligations and requirements to those required by the *FIPPA*. However, the primary goal of the ISA is to ensure that City, and any organization the City is sharing information with, complies with applicable privacy legislation.

In general, an ISA should include or address the following:

1. A statement of the purpose(s) for the disclosure or sharing of the personal information.

2. The legal authority to disclose or share personal information for the above purpose(s).

3. The legal authority for the collection of the personal information by the City or the organization to which that information is being disclosed.

4. A description of the personal information that will be disclosed, that is as specific and comprehensive as possible in the circumstances (eg. the nature and type of personal information, the quantity of personal information, etc.).

5. A description of how the personal information will be disclosed (eg. continuously via electronic database, on demand via e-mail, etc.).

6. If possible, a description of who within the City or organization will have access to the personal information and any other disclosure restrictions.

PRIVACY MANAGEMENT POLICY
Council Policy No. 140/19

SCHEDULE A

INFORMATION SHARING AGREEMENT GUIDELINES

7. A description of the authorized use of the personal information and limits on further use of that information.

8. A clear statement about who has custody and control of the personal information.

9. An undertaking by the City and/or organization to protect the information in a certain manner (ie. physical safeguards, etc.).

10. An undertaking that the personal information will be stored within Canada except as otherwise permitted by the *FIPPA*.

11. A description of the process to ensure accuracy of the personal information, including the process to update and correct personal information if needed.

12. A specific retention period (in accordance with *FIPPA* and the Policy) and directions on destruction when the retention period expires.

13. A description of the process for managing privacy breaches, complaints, reporting, and incidents.

14. Methods for monitoring compliance with the ISA and consequences of non-compliance.

15. The Term of the ISA and process for amendment or renewal.

All ISAs, to which the City is to be a party, should be reviewed by the Head prior to being signed, and as directed by the Head, by legal counsel.