

City of St. John's Corporate and Operational Policy Manual

Procedure Title: Personal Information and Record Protection Procedures	
Authorizing Policy: Privacy Management Policy	
Procedure #: 01-04-02-01	
Last Revision Date: N/A	Procedure Sponsor: City Clerk

1. Procedure Statement

This procedure outlines the City's specific requirements for collecting, using, disclosing, and protecting Personal Information. These requirements ensure the City has appropriate safeguards that will support transparent and informed consent and protect Personal Information against loss or theft, as well as unauthorized access, disclosure, copying, use, modification, or disposal.

2. Definitions

"Department Head" means any Employee reporting directly to the City Manager and/or Council.

"Office of the Information and Privacy Commissioner" (OIPC) means the Office of the Information and Privacy Commissioner of Newfoundland and Labrador.

"Personal Information" shall have the same meaning as defined by Section 2(u) of ATIPPA, that is, "Recorded information about an identifiable individual, including:

- i. the individual's name, address or telephone number,
- ii. the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- iii. the individual's age, sex, sexual orientation, marital status or family status,
- iv. an identifying number, symbol or other particular assigned to the individual,

- v. the individual's fingerprints, blood type or inheritable characteristics,
- vi. information about the individual's health care status or history, including a physical or mental disability,
- vii. information about the individual's educational, financial, criminal or employment status or history,
- viii. the opinions of a person about the individual, and
- ix. the individual's personal views or opinions, except where they are about someone else."

"Record" shall have the same meaning as defined by Section 2(y) of the ATIPPA, that is, "a record of information in any form, including a dataset, information that is machine readable, written, photographed, recorded, or stored in any manner, but does not include a computer program or a mechanism that produced records on any storage medium."

3. Procedure Requirements

3.1 Collection of Personal Information

The City shall only collect Personal Information that is required to administer its programs and services, or to comply with municipal, provincial, or federal legislation. Such collection shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is collected.

When collecting Personal Information, Employees shall collect Personal Information directly from the individual to whom the information relates, with limited exceptions as authorized by ATIPPA and:

- a) Prior to collection and use, or at the time of collection, provide notice or obtain the necessary consent as prescribed by the ATIPPA. Consent shall be in writing, where possible;
- b) Inform individual(s) of the legal authority under which the information is being collected. This information shall be included on all City forms where Personal Information is being collected;
- c) State the purpose(s) for which the Personal Information is to be used; and
- d) Provide the title, business address, and business telephone number of an Employee who can answer questions about the Personal Information collection.

To support the commitment to transparent and informed consent, revisions to existing forms and all new forms shall be forwarded to the ATIPP Coordinator prior to being implemented.

3.2 Protection of Personal Information

Department Heads shall oversee the development and implementation of a Records Safeguard Plan to support appropriate safeguards for departmental Records (including electronic Records) containing Personal Information, including any Records managed by third parties.

The ATIPP Coordinator shall provide Department Heads with a Records Safeguard Plan template. Department Heads shall provide the ATIPP Coordinator with their department's completed plan, which shall include:

- a) A description of the administrative, technical, access control, and physical safeguards in place for departmental Records containing personal information.
- b) A description of any deficiencies in existing safeguards and plans to mitigate them.

Additional information is available in the **Records Safeguard Plan Guidelines**. If requested, the ATIPP Coordinator shall work with the departmental staff to support the development of the plan. The ATIPP Coordinator may follow up with the Department Head if other deficiencies beyond those identified are apparent upon review of the plan.

A revised and updated Records Safeguard Plan shall be completed as directed by the ATIPP Coordinator.

3.2.1 Protection of Privacy Standards

To ensure appropriate protection of privacy, the following minimum standards shall apply. There may be other requirements identified during the development of the Records Safeguard Plan that are necessary to appropriately protect departmental/divisional information.

- a) Accessing Personal Information shall be restricted to only those Employees requiring access to carry out their duties.
- b) Personal Information shall not be disclosed to members of the public, Members of Council, or other Employees (outside of its intended use)

without the consent of the individual to whom the information relates, or in accordance with legislation.

- c) Personal Information shall not be discussed in public areas where it may be overheard by others who are not authorized to have such information.
- d) Individuals shall lock computer screens when not in use and shall ensure physical Records containing Personal Information are secure when not in use.
- e) Records containing Personal Information shall not be removed from City worksites, unless required to complete duties and responsibilities of the position.
- f) If documents are opened or reviewed in public places, the Personal Information contained in the Records shall be protected unless otherwise authorized.
- g) System, software, and/or email passwords allowing access to Personal Information shall not be shared or disclosed to others.
- h) Cabinets or storage locations containing Personal Information or confidential information shall be secured at the end of each day or when not in use.
- i) External storage devices, such as USB sticks or external drives, shall be appropriately protected by being locked in a drawer or cabinet and/or being password encrypted.
- j) Keys to secure storage areas shall not be left in open places.
- k) Documents containing Personal Information or confidential information shall be retrieved from printers or fax machines in a timely manner.
- l) Destruction of Personal Information shall be done by placing such documents in secure shredding bins or erasing digital storage devices. Records or digital storage devices shall not be placed in the garbage or in regular recycling bins.
- m) When a meeting is completed, all Personal Information or confidential materials shall be removed from the room, erased from boards and flipcharts, and all users shall sign out of computers.
- n) Records containing Personal Information stored on shared computer networks shall be restricted to secure directories providing access only to authorized individuals.

4. Application

This procedure applies to (i) all Members of Council; (ii) all Employees; and (iii) all Records containing Personal Information in the custody and/or under the control of the City of St. John's.

5. Responsibilities

5.1 ATIPP Coordinator is responsible for:

- a) Providing Department Heads with a Records Safeguard Plan template and providing support, as requested, for plan completion; and
- b) Monitoring departmental plan commitments for any mitigation measures.

5.2 All Members of Council and all Employees are responsible for:

- a) Safeguarding the privacy and security of information in the workplace and when working remotely.

5.3 Department Heads are responsible for, in addition to the duties noted in Section 5.2:

- a) Ensuring there are appropriate security arrangements for Personal Information in their department's custody;
- b) Providing the ATIPP Coordinator with their department's completed Records Safeguard Plan; and
- c) Ensuring commitments for any mitigation measures are implemented.

6. References

- [Access to Information and Protection of Privacy Act, 2015](#)
- 01-04-02 Privacy Management Policy
- Records Safeguard Plan Guidelines

7. Approval

- Procedure Sponsor: ATIPP Coordinator
- Procedure Writer: ATIPP Coordinator / Policy Analyst
- Date of Approval from:
 - Corporate Policy Committee: November 13, 2018
 - Senior Executive Committee: May 24, 2019

8. Monitoring and Contravention

The ATIPP Coordinator shall monitor the application of this procedure.

Any contravention of the procedure shall be brought to the attention of the Department of Human Resources, the Office of the City Solicitor, the City Manager, and/or the OIPC for further investigation and appropriate action, which may include, but is not limited to legal action and discipline, including dismissal.

9. Review Date

Every 3 years