TOWN OF BRIDGEWATER
PRIVACY BREACH MANAGEMENT POLICY

POLICY NO. 122

Purpose

The Town of Bridgewater ("Town", "organization") makes every effort to protect the privacy, confidentiality and integrity of the Confidential Information entrusted to its care. This policy has been adopted to demonstrate the Town's commitment to promptly investigate, contain, and mitigate any Privacy Incident that has or may lead to a Privacy Breach.

Scope

This policy applies to any Town employees as well as third-party Service Providers engaged by the Town to foster an environment where Town Staff are vigilant and proactive with respect to safeguarding Confidential Information, which includes Personal Information. It is the responsibility of every employee of the Town to be aware of this policy and the associated Privacy Breach Management Protocol and to conduct their work-related activities accordingly.

Notification

Where the Town has determined in the circumstances that it is reasonable to believe a Privacy Incident has occurred and creates a real risk of significant harm to an individual or third party[1], notification will be provided to affected individuals, third party, and/or the Information and Privacy Commissioner of Nova Scotia. The Town shall notify the affected individual(s) or third party, using appropriate direct and indirect means as soon as feasible after it confirms that the Privacy Breach has occurred.

Policy Statement

All Town Staff are required to immediately notify their Supervisor of any actual or suspected Privacy Incident – including events that involve or affect Confidential Information of Third Parties. The Supervisor must notify the Privacy Officer of the Privacy Incident within 24 hours with details of the incident. The notification can be verbal, in person, in writing or in an electronic or digital format. The Privacy Officer will follow the Town's Privacy Breach Management Protocol to initiate an appropriate follow up.

---

[1] While a Privacy Breach will likely involve more than one person, note that the legislative requirement applies even in the case of a sole person being an Affected Individual. For an evaluation regarding the criteria of "Real Risk of Significant Harm" please refer to Appendix C in the Privacy Breach Management Protocol.

If a staff member wishes to report a suspected Privacy Incident confidentially, the Privacy Officer can receive the information directly and will not disclose the identity of the staff beyond a need to know basis without the staff's consent, unless required by law. The Town commits to protecting employees against reprisal when they have made a report in good faith. This includes protecting the employee making the report and other persons involved in the Privacy Incident situation by keeping records separate from existing files and revealing information only to the investigator or the senior officer.

Definitions

For the purposes of this Policy and Protocol, **Compromise of Confidential Information** means:

1. Any failure to adhere to the Town's Personnel Policy & Procedures Manual concerning the collection, processing, protection or sharing of Personal Information and/or adherence to privacy and security policies as they may be developed.
2. Any unauthorized access to, collection, use or disclosure of Personal Information by Town Staff.
3. Any breach of a contractual (e.g. non-disclosure or data sharing agreement) agreement for the handling of Personal Information.
4. Any circumstances where Personal Information is stolen, lost or subject to any unauthorized use or disclosure or where records of Personal Information are subject to unauthorized copying, modification, or disposal.

Confidential Information means information as defined in Nova Scotia's *Municipal Government Act*, Part 20 - *Freedom of Information and Protection of Privacy,* section 481(1) relating to third parties. Confidential Information is also the information defined in sections 472 through 479(A) of the Act relating to the Town's relations with other governments, meetings in camera, advice or recommendations, law enforcement, solicitor-client privilege, financial or economic interests, health and safety, conservation, or labour relations. For the purposes of this policy, Confidential Information also includes Personal Information.

Personal Information as defined in the Act, section 461, means recorded information about an identifiable individual including (but is not restricted to):

(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 history, including a physical or mental disability,
(vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,
(viii) anyone else's opinions about the individual, and
(ix) the individual's personal views or opinions, except if they are about someone else.

Privacy Breach means any event where it has been established on a balance of probabilities that a Compromise of Confidential Information has occurred.

Privacy Incident means any event where a Compromise of Confidential Information is believed to have occurred, but a Privacy Breach has not been established.

Service Provider means an (i) individual, company, or other entity or (ii) employees of a company or other entity that have entered an agreement to provide services to the City.

Review Schedule

This Policy and associated Protocol will be reviewed no later than every twenty-four (24) months and updated as required.

Approved: April 27, 2026 Motion#: 26-075