TOWN OF BRIDGEWATER
POLICY
OPEN SMART COMMUNITY PILOT

Policy No.	**103**
Approved:	September 28, 2020
Resolution #:	20-193

1. Purpose

1.1 The Town of Bridgewater desires to be an "open smart community". We recognize the growing interest in, and value of, open smart community approaches to municipal governance and service delivery, as exemplified by the Energize Bridgewater program. At the same time, the Town recognizes that emerging smart cities technologies usually associated with these approaches have the potential to erode privacy rights, exacerbate social inequalities, introduce security and procurement risks, and create other challenges for the organization and the community. This policy establishes a framework to guide future decision-making and further policy development on this topic, to enable the safe and appropriate adoption of smart cities technologies and practices and the management of community data, while at the same time reducing risks to the organization and the community.

1.2 Short-term objectives of this Policy:

- Establish baseline principles and practices to guide decision-making related to the management of community data and the safe adoption of smart cities technologies;
- Lay out a roadmap for the development of further policies related to the management of community data and the safe adoption and deployment of smart cities technologies;
- Establish accountability processes and structures related to the management of community data and the safe adoption of smart cities technologies;
- Align political and administrative objectives related to the management of community data and the safe adoption of smart cities technologies;
- Improve transparency in the Town's position on matters related to the management of community data and the safe adoption of smart cities technologies.

1.3 Long-term objectives of this Policy:

- Improve citizen access to, and control over, the governance of community data;
- Increase digital literacy of citizens and equitable participation in the digital economy;
- Ensure citizen trust towards data collected and used by the Town of Bridgewater;

- Ensure adherence to Provincial privacy protection laws, including Part XX (Freedom of Information and Protection of Privacy) of the *Municipal Government Act*, and access to information laws and related best practices;
- Ensure the security and reliability of municipal data and IT systems;
- Ensure citizen-centric approaches and transparency when sourcing IT solutions;
- Ensure interoperability, interchangeability, and market fairness when sourcing IT solutions;
- Strengthen municipal control over public domain technologies and regulations that relate to privacy;
- Stimulate innovation and economic development through the appropriate use of community data.

1.4 This policy has been approved on a pilot basis. During the pilot, this policy will be evaluated for its strengths and weaknesses, as well as the administrative impact of its implementation. Continuation past the pilot phase is subject to a positive evaluation.

2. Scope

2.1 This policy applies to all Town of Bridgewater departments and operations.

3. Definitions

3.1 An **open smart community** is defined as one where one where residents, civil society, academics, and the private sector collaborate with public officials to mobilize data and technologies when warranted in an ethical, accountable and transparent way to govern the community as a fair, viable and liveable commons and balance economic development, social progress and environmental responsibility. (Reference: OpenNorth)

3.2 An **emerging smart cities technology** is defined as one that makes use of any or a combination of the following technologies:
- Participatory use of connected technologies, where many users generate large volumes of data;
- Public and private urban surveillance systems connected to the internet;
- Internet of things (IoT);
- Artificial intelligence (AI) or machine learning;
- Community data that is analysed through computer algorithms and may be subject to algorithmic bias;
- Mass collection of personal information including but not limited to personal, biometric, genetic, and health data;
- Open data;
- Big data.

3.3 An **algorithm** is defined as a sequence of instructions, rules, and calculations executed by a computer in a particular order to yield a result, typically an answer to a specified problem. Algorithms can be used in combination with other algorithms to solve complex problems. (Reference: Brookfield Institute)

3.4 **Artificial Intelligence (AI)** is defined as computer programs capable of behaviour commonly thought to require intelligence. (Reference: Brookfield Institute)

3.5 **Big data** is defined as a dataset with a size beyond the processing capability of a typical database for the purpose of data capture, storage, management, and analysis. (Reference: Brookfield Institute)

3.6 The **internet of things (IoT)** is defined as a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. (Reference: Wikipedia)

3.7 **Machine learning** is defined as a technique that enables computer systems to learn and make predictions based on historical data. (Reference: Brookfield Institute)

3.8 **Municipal data** is defined as records and information generated, collected, retained, used, and disclosed by the Town of Bridgewater for any purpose related to the Town's operations and activities.

3.9 **Open Data** is defined as structured data that is machine-readable, freely shared, used and built on without restrictions. (Reference: Government of Canada)

3.10 **Personal information** is defined as recorded information about an identifiable individual, as described in Section 461(f) of the *Municipal Government Act of Nova Scotia*.

3.11 The **Privacy Officer** is an individual appointed by Bridgewater Town Council to have oversight and accountability over the Town's privacy policies, and the implementation of those policies. The Privacy Officer's responsibilities are subject to the privacy provisions of the *Municipal Government Act.*

3.12 A **Privacy Impact Assessment (PIA)** is defined as a process that helps determine whether government initiatives involving the use of personal information raise privacy risks; whether the government measures, describes, and quantifies these risks; and whether it proposes solutions to eliminate privacy risks or mitigate them to an acceptable level. (Reference: Brookfield Institute)

3.13 A **Threat and Risk Assessment (TRA)** is defined as a process of identifying system assets and how these assets can be compromised, assessing the level of risk that threats pose to assets, and recommending security measures to mitigate threats. (Reference: Government of Canada)

4. Guiding Principles

Interpretation of this Policy, and development of future open smart community policies and procedures shall align with the following guiding principles (Reference: OpenNorth):

4.1 **Accountable governance**: governance of open smart community initiatives should be ethical, accountable, and transparent. This applies to the governance of social and technical platforms which includes data, algorithms, skills, infrastructure, and knowledge. The Town affirms that all municipal data is the property of citizens, not municipal

departments. Information collected and generated is subject to the access to information provisions of the *Municipal Government Act*.

4.2 **User-centered**: recognize that technology should be built for purpose and designed with the user in mind and the problem that it intends to solve. Particular focus needs to be applied to the user experience of marginalized community members.

4.3 **Participatory, inclusive, and responsive:** government, civil society, private sector, the media, academia and residents should meaningfully participate in the governance of open smart community initiatives and have shared rights and responsibilities. This entails a culture of trust and critical thinking and fair, just, inclusive and informed approaches. Policies and programs should empower and connect groups inside and outside government, especially marginalized groups.

4.4 **Interoperability & transparency**: data and technologies should be fit for purpose, able to be repaired and queried, have open source code, adhere to open standards, be interoperable, durable, secure, and where possible locally procured and scalable. Data and technology should be used and acquired in such a way as to reduce harm and bias, increase sustainability and enhance flexibility. If automated decision-making is used, these systems should be designed to be legible, responsive, adaptive and accountable.

4.5 **Privacy & control**: privacy is a fundamental right, data management should be the norm, and custody and control over data generated by smart technologies should be held and exercised in the public interest. Data governance includes sovereignty, residency, security, individual and social privacy, grants people authority over their personal data, and is open by default. The collection, use, disclosure, retention, and security of personal information is governed by the privacy provisions of the *Municipal Government Act.*

4.6 **Resilient & adaptive**: prioritize the well-being of citizens, enhance local ability to reduce impact to the natural environment, and increase the community's capacity to respond to economic and physical disruptions.

4.7 **Appropriate use of technology**: data and technology are not the solution to many of the systemic issues the community faces, nor are there always quick fixes. Such problems require innovative, sometimes long term, social, organizational, economic, and political processes and solutions. Emergent smart city technologies, in particular, should only be applied once community problems or needs have been thoroughly assessed through democratic processes to be priorities in need of solutions, and only after non-technological solutions have been considered. When emergent smart city technology solutions are applied, they should optimize the use of resources to improve the effectiveness and reduce the costs of providing municipal services and other government operations.

5. Application of Policy

5.1 This Policy shall provide guidance in the development of further policies and procedures as described in section 6 (Implementation).

5.2 This Policy shall be triggered and used for guidance any time a policy, procedure, or project that is proposed or implemented by the Town of Bridgewater has an emergent smart cities technology associated with it.

6. Implementation

Further open smart community policies and procedures shall be established as outlined below:

6.1 Accountability Structures and Roles:

6.1.1 The Town shall establish a Data Governance Committee that will lead the development of further open smart community policies and procedures, and monitor the implementation and evaluation of these activities. The Committee will begin as an internal staff committee, with the goal of transitioning to a multi-stakeholder Committee of Council, including citizen representation, in 2021. As part of its mandate, the Committee will assess the need for, and implement the following as appropriate:

- Additional data governance or advisory structures for the Energize Bridgewater program as well as future open smart community initiatives;
- An independent governance or advisory structure for municipal Open Data systems.

6.1.2 The Town shall appoint a Chief Security Officer (CSO), who shall oversee information security related issues. The role description of the CSO shall be informed by best practices and all applicable legislation.

6.2 Privacy:

6.2.1 The Town shall develop and adopt a Privacy Policy that is informed by best practices, and that conforms to all applicable privacy legislation. The Policy shall include, but not be limited to the following:

- Privacy & security breach protocols;
- A privacy policy review framework;
- A process whereby Senior Management can provide privacy related oversight for open smart community initiatives;
- Measures to bolster staff education and awareness of privacy, both at the time of hiring and annually. Privacy training should be updated to reflect changes in best practices and legislation, and will have versions tailored to staff who work directly with personal information;
- Measures to monitor compliance with privacy-related policy and legislation;
- The development of a Personal Information Inventory, which enables the ongoing tracking of all personal information that is collected and retained by the Town;
- An external communications process to notify individuals when their data is being used or disclosed, and bolster communication materials informing individuals of how to submit a complaint regarding privacy-related compliance;

- Requirements to involve the Privacy Officer during the design stage of new services or programs to consider privacy at the onset;
- Requirements for the completion and maintenance of a Threat and Risk Assessment (TRA) and Privacy Impact Assessment (PIA) for all projects that involve personal information.

6.2.2 The Privacy Officer shall develop a plan for reviewing the Town's overall privacy management framework, including formal measures and a schedule for when each policy or control is reviewed. The Privacy Officer will periodically review all privacy-related controls (including, but not limited to, privacy-related policies and procedures, training, and service agreement templates) in use at the Town, to ensure that they are complete, effective, based upon current best practices, addressing issues identified by audits, supported by training, supported by formal policies and procedures, and requiring documentation of all issues that are encountered and addressed.

6.3 Data Management:

6.3.1 The Town shall increasingly adopt an "open by default" stance on all data collected by the municipality. This means that data management policies, protocols, and procedures have the aim of making municipal data accessible to the public while also adhering to relevant policy, legislation and leading practices related to the privacy and security of personal information. In alignment with Guiding Principle 4.5 (Privacy & Control), the Town shall ensure that in moving toward open use of data, the following data types shall remain secure and protected:

- Personal information;
- Data that, if disclosed, may compromise public safety or protection of property;
- Critical infrastructure and operations data including IT systems;
- Data for which the Town does not hold intellectual property or the right to republish;
- Third-party trade secrets;
- Any data protected by specific laws and regulations.

6.3.2 The Town shall develop and adopt an Open Data Policy that is informed by best practices, and that conforms to all applicable privacy legislation. The Policy shall include, but not be limited to the following:

- The requirement for oversight by an independent, multi-stakeholder governance committee;
- A prioritized list of datasets to publish.

6.4 Information Security:

6.4.1 The Chief Security Officer shall oversee the Town's information security policies and practices.

6.4.2 The Town shall systematically assess and harden the security of all its IT systems and strive to follow international standards and practices on this matter. This shall pertain to both virtual and physical security. Priority shall be given to the hardening of systems that collect, store, and transmit personal information and critical infrastructure and operations data.

6.4.3 That Town shall maintain and strengthen measures to bolster staff education and awareness of IT security, both at the time of hiring and annually.

6.4.4 Threat and Risk Assessments (TRA) and Privacy Impact Assessments (PIA) shall continue to be conducted for all systems containing personal and/or confidential information. Any IT systems that are newly implemented or adopted are required to conduct a TRA.

6.5 Procurement:

6.5.1 The Town shall assert its control and ownership of all data collected by or for its programs and operations regardless of who has custody of it, through schedules within the contracts and agreements that it signs with all partners and service providers.

6.5.2 The Town shall develop and include a Privacy Protection Schedule in contracts signed with third-parties, to ensure that the privacy and confidentiality of all information is maintained by all non-Town of Bridgewater program members. The Schedule shall include timelines for privacy and security breach notification, require that contractors receive privacy training if they are dealing with personal information, and require that contractors undergo and cooperate with privacy-related audits of their services.

6.5.3 All procurement that involves IT systems and/or emerging smart cities technologies shall be vetted by the Director of IT Services.

6.5.4 All vendors lobbying for products and services related to IT systems and/or emerging smart cities technologies shall be referred to the Director of IT Services. In alignment with Guiding Principle 4.7 (Appropriate use of technology), unsolicited lobbying by these vendors shall be discouraged by implementing a “don’t call us, we’ll call you” practice.

6.5.5 The Town shall develop and implement Public Open Standards for IT development and procurement aimed to maximize the public good. These standards may include but are not limited to requirements for:

- Interoperability of IT systems and data;
- Promotion of open procurement practices such as neutral market assessments;
- Public participation in IT systems development and testing;
- Terms of access that allow public use of standardized technologies;
- Vendor-neutrality;

- Avoidance of vendor lock-in;
- Decentralized data interoperability and portability across discrete systems and applications.

6.5.6 The Town shall develop and implement cybersecurity standards for IT development and procurement to ensure that IT technologies and infrastructures are protected from being hacked via a cyberattack and that data are protected from improper access and for privacy. These standards shall consider security requirements for system components, architectures, operations, communications systems, and data protection.

6.5.7 All code developed for the Town shall become exclusive property of the Town, to allow for later release under Open Source licenses, if desired.

7. Policy Administration

7.1 Administration of this policy shall be the responsibility of Senior Management, under the oversight of the CAO.