



TOWN OF POUCH COVE

ELECTRONIC MOBILE DEVICE USE POLICY

1. BACKGROUND

Mobile devices such as smartphones, tablets, and laptops have become essential tools in supporting communication, service delivery, and flexible work arrangements within Newfoundland and Labrador Municipalities including the Town of Pouch Cove. These devices, whether Town-issued or personal, allow approved employees, elected officials, and volunteers to access Town systems, respond to inquiries, and manage responsibilities remotely and in real time. However, using mobile devices in uncontrolled environments, such as homes, vehicles, or public spaces, comes with added risks; such as privacy breaches, unauthorized access to Town systems or emails, using unsecured Wi-Fi, and potentially losing data due to device theft, loss, or viruses. Mobile devices present greater challenges to protecting Town data than desktop computers in offices, especially when they are used to access or store confidential or personal information. Despite the risks, mobile devices offer many benefits, like flexibility, faster communication, and increased productivity if used properly. As such, the Town has created this policy in order to help Town users balance the efficiency benefits of mobile technology with the responsibility to protect information, comply with legislation, and maintain public trust.

2. PURPOSE

This policy describes how the Town of Pouch Cove uses electronic mobile devices such as smartphones, tablets, and laptops to support communication, access information, and perform the work required for each person's role, while further aiming to manage mobile device use to ensure the protection of Town information and support privacy, security, and service delivery. It provides practical, secure, and responsible guidance for Town users regarding access and management of Town related information via electronic mobile devices, and supports compliance with applicable legislation, including but not limited to the *Towns and Local Service Districts Act*, the *Access to Information and Protection of Privacy Act 2015*, and the *Municipal Conduct Act*.

3. SCOPE

This policy shall apply to all employees, elected officials, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons working on behalf of the town (hereafter referred to as "Town Users").

4. DEFINITIONS

- 4.1 Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015)** is the provincial legislation that governs access to public records and the collection, use, disclosure, protection, and retention of all personal information by public bodies in Newfoundland and Labrador. It establishes requirements to ensure transparency while safeguarding individuals' privacy
- 4.2 Archive** shall refer to records that have been determined to possess enduring administrative, legal, fiscal, evidential, or historical value and are preserved for long-term or permanent retention
- 4.3 CAO** shall refer to the Chief Administrative Officer of the Town of Pouch Cove
- 4.4 Compliance** shall refer to the set of activities and processes that result in meeting and adhering to applicable legislation, rules, and codes of professional conduct, as well as the Town's policies and procedures

4.5 Confidential information shall refer to information in the custody and/or control of the Town that is prohibited from disclosure pursuant to legislation or court order or any other information that pertains to the business of the Town generally considered to be of a confidential nature, including, but not limited to:

- 4.5.1 Any matter that falls under the exceptions to disclosure identified in the Access to Information and Protection of Privacy Act (ATIPPA, 2015), whether or not a request for access has been made,
- 4.5.2 Personal information which would constitute an unreasonable invasion of privacy,
- 4.5.3 Potential acquisitions or disposition of real property,
- 4.5.4 Information which would reveal the substance of deliberation of a closed meeting,
- 4.5.5 Pending contracts including tenders, requests for proposals (RFPs), and records related to potential procurement,
- 4.5.6 Draft documents and legal instruments including reports, policies, bylaws, and resolutions that have not been the subject matter of deliberation in a meeting open to the public,
- 4.5.7 Employment and collective bargaining matters,
- 4.5.8 Legal matters,
- 4.5.9 Law enforcement matters.

4.6 Council shall refer to the Town Council continued or incorporated under the TLSDA

4.7 Councillor shall refer to and include a Mayor and a Councillor of a Town Council

4.8 Employee or Employees shall refer to any individual under an employment contract with the Town of Pouch Cove including all members of staff, volunteers, contractors, all members of the Pouch Cove Volunteer Fire Department, and all members of Town Council

4.9 Mobile Device shall refer to any small, portable computing device which can access, store, and/or send information. Mobile devices run on batteries, connect to wireless networks, and can access email, files, and other systems. Examples include but are not limited to: smartphones, tablets, and laptops

4.10 Multi-Factor Authentication (MFA) shall refer to a security measure that requires users to verify their identity using two or more authentication factors, such as a password and a one-time code, biometric verification, or an authentication app, before granting access to a mobile device or organizational resources. MFA helps protect against unauthorized access if a password is compromised

4.11 Municipality shall refer to the Town of Pouch Cove and shall include all departments, boards, committees, agencies, employees, elected officials, contractors, volunteers, and the Pouch Cove Volunteer Fire Department, acting on behalf of the Town

4.12 Network shall refer to a group of connected computers or devices that share data and resources. Networks can be wired or wireless, communicating between users, systems, and services

4.13 Personal Identifiable Information (PII) shall refer to recorded information about an identifiable individual, as defined under applicable privacy legislation, including:

- 4.13.1 the individual's name, address, or telephone number,
- 4.13.2 the individual's race, national or ethnic origin, religious or political beliefs or associations, or skin colour
- 4.13.3 the individual's age, sex, sexual orientation, marital status, or family status,
- 4.13.4 an identifying number, symbol or other particular assigned to the individual,
- 4.13.5 the individual's fingerprints, blood type or inheritable characteristics,
- 4.13.6 information about the individual's health care status or history, including any disability,
- 4.13.7 information about the individual's educational, financial, criminal, or employment history,
- 4.13.8 the opinions of a person about the individual, and
- 4.13.9 the individual's personal views or opinions, except where they are about someone else

- 4.14 Record** shall refer to any recorded information, regardless of physical form or characteristics, created, received, maintained, or used by the Town in the conduct of municipal business and which provides evidence of activities, decisions, transactions, and/or legal obligations
- 4.15 Records Retention and Disposal Schedule (RRDS)** shall refer to the approved corporate schedule that establishes the minimum retention periods, disposition requirements for municipal records, and how they will be archived or disposed of at the end of their lifecycle
- 4.16 Smartphone** shall refer a mobile phone that works like a small computer. It allows users to make and receive calls, send and receive text messages, send and receive emails, browse the internet, and access files
- 4.17 Town** refers to the Town of Pouch Cove.
- 4.18 Town Manager/Clerk** shall refer to a Town Clerk responsible for the day-to-day administrative activities of the Town
- 4.19 Town Users** shall refer to all employees, elected officials, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties, and any other persons working on behalf of the Town
- 4.20 Virtual Private Network (VPN)** shall refer to technology which encrypts data during transmission, ensuring secure communication over potentially unsecured networks

5. POLICY STATEMENTS

5.1 Town Issued Mobile Devices

- 5.1.1 The Town provides mobile devices based on job roles and responsibilities
- 5.1.2 Town-issued devices are configured and managed by the Town and are used exclusively for Town-related work and responsibilities
- 5.1.3 All information created and/or stored on these devices is managed in accordance with the Town's Records Management Policy
- 5.1.4 Town records are stored in the Town's official shared drive or other designated repository
- 5.1.5 Town users shall use caution when visiting websites, opening file attachments, or clicking links sent in emails and/or text messages
- 5.1.6 Town-issued devices are not used for personal or commercial activities
- 5.1.7 Town users shall not permit any friends, family members, or other unauthorized third parties to use Town-issued devices
- 5.1.8 Town users return the Town-issued devices at the end of their employment or elected term

5.2 Personal Mobile Devices

- 5.2.1 Personal devices are used for Town business with approval from the CAO/Town Clerk
- 5.2.2 Approved personal devices follow the same security expectations as Town-issued devices
- 5.2.3 Town related information is accessed using secure tools and is not stored in personal cloud accounts or any unapproved apps
- 5.2.4 Secure data backup practices are in place for personal devices used to support Town work
- 5.2.5 Town data is deleted from personal devices during offboarding

5.3 Device Security

- 5.3.1 Town users apply strong passwords, or biometric protection, and enable screen locking on all devices. MFA is used to gain access to Town accounts, apps, and systems
- 5.3.2 Town users shall never share log-in credentials, passwords, and/or PIN with any other persons
- 5.3.3 All devices are to be automatic screen lock and encryption enabled to ensure the device(s) lock when unattended
- 5.3.4 Town users shall use only trusted USB devices, chargers, and/or power adapters, and shall refrain from connecting to any public, shared, and/or other non Town-issued devices
- 5.3.5 Connections to public Wi-Fi are made using secure methods such as VPN
- 5.3.6 Approved apps and secure channels are used for accessing and/or sharing Town information

- 5.3.7 Software updates and antivirus protection are maintained where applicable
- 5.3.8 Town users use caution when clicking links in emails and/or text messages, opening file attachments, and browsing websites
- 5.3.9 Town users activate device location services such as “Find My iPhone” (iOS) or “Find My Device” (Android) to help locate the device and/or remotely wipe any data in instances where the device is lost and/or stolen.

6. INCIDENT REPORTING PROCEDURE

- 6.1.1 Lost and/or stolen devices are reported promptly to the CAO/ Town Clerk
- 6.1.2 Any unusual activity and/or unauthorized access is reported to the CAO/Town Clerk and/or ATIPP Coordinator as is appropriate
- 6.1.3 Responses to incidents follow the Town’s Privacy and IT Guidance
- 6.1.4 Records of reported incidents are managed appropriately in accordance with the Town’s Record Management Policy
- 6.1.5 Refer to chart below for further details on reporting procedures regarding this policy:

Situation	Immediate Action	Report To
Device lost or stolen	Notify Town Clerk/CAO within 24 hours	Town Clerk/CAO
Suspicious login or account access	Change password and report immediately	IT or ATIPP Coordinator
Personal device compromise (e.g., virus)	Disconnect from Town systems; notify supervisor	Town Clerk/CAO
Unauthorized access to Town info	Report breach and preserve evidence	ATIPP Coordinator

6.2 Offboarding Procedure

- 6.2.1 Town users must return all Town-issued electronic devices to the CAO/Town Clerk at the end of their employment or elected term
- 6.2.2 All Town data stored on personal devices must be permanently deleted at the end of their employment or elected term
- 6.2.3 Ensure that all access to Town systems, email, internal software, and shared drives is revoked and/or disabled at the end of their employment or elected term

7. ROLES AND RESPONSIBILITIES

7.1 ATIPP Coordinator shall ensure that access to information requests and information protection obligations are fulfilled in accordance with the *ATIPP Act, 2015*, particularly when electronic devices are used to create, store, and/or access municipal records in while:

- 7.1.1 Receiving and processing requests made under the ATIPP Act, 2015
- 7.1.2 Coordinating responses to requests for approval by the head of the public body (as designated under s. 109 of the ATIPP Act, 2015)
- 7.1.3 Communicating, on behalf of the Town, with applicants and third parties regarding requests throughout the process including the final response
- 7.1.4 Educating Town users of the public body about the applicable provisions of ATIPP Act, 2015
- 7.1.5 Tracking requests made under ATIPP Act, 2015 and the outcome of the request
- 7.1.6 Preparing statistical reports regarding requests for the head of the public body

7.2 Chief Administrative Officer (CAO)/Town Clerk

- 7.2.1 Overall management of the Town's records and technology tools
- 7.2.2 Organize orientation and training for Town Users regarding their records management responsibilities, including secure mobile device use and privacy obligations
- 7.2.3 Provide tools and resources to Town Users to support compliance with this policy, (ie. secure storage locations, VPNs, approved applications)
- 7.2.4 Authorize/issue equipment and tools to Town Users for the production/storage of town records (ie. Town network and/or email account, computing devices, cellular phone)
- 7.2.5 Authorize and issue Town equipment and access credentials (ie. Town network, mobile devices, email accounts)
- 7.2.6 Approve secure storage or use of Town data offsite (ie. approved home offices)
- 7.2.7 Control and monitor access to Town records and digital assets
- 7.2.8 Retrieve, review, and catalogue records and devices returned during offboarding
- 7.2.9 Support secure disposal of records and device decommissioning as per the RRDS
- 7.2.10 Identify alternative storage locations for Town records including third party storage and/or archives where necessary
- 7.2.11 Advise Town Council of any risks and/or non-compliance issues related to device use and/or information handling

7.3 Town Users

- 7.3.1 Use Town-issued or approved personal mobile devices in accordance with this policy
- 7.3.2 Protect the security and confidentiality of Town information accessed, stored, or transmitted via mobile devices in accordance with *ATIPPA, 2015*
- 7.3.3 Report incidents (ie. lost/stolen devices, suspected privacy breaches) within required timeframes and in accordance with this policy
- 7.3.4 Participate in onboarding, annual refresher, and any other offered training pertaining to secure device use and privacy
- 7.3.5 Ensure that Town data is removed from personal devices and that all Town-issued devices are returned upon offboarding

7.4 Town Council

- 7.4.1 Approves and authorizes this policy and any updates
- 7.4.2 Promotes adherence to ethical and secure use of electronic devices by all Town Users
- 7.4.3 Ensures the Town's electronic records systems are adequately resourced and supported
- 7.4.4 Designates the head of the public body for the Town in accordance with s. 109 of the *ATIPP Act, 2015*. This person cannot also be the ATIPP Coordinator.

8. MONITORING AND COMPLIANCE

The Town of Pouch Cove updates this policy as needed to accommodate changes in the business environment, legislation, and technology. Compliance with this policy is mandatory for all Town Users. Non-compliance may result in the revocation of device and/or system access, disciplinary action up to and including termination, and/or referral to law enforcement or other authorities, where appropriate. In accordance with s. 64 of the *ATIPP Act, 2015*, the Town has a legal duty to protect personal information under its custody or control. Misuse of Town-issued devices or unauthorized access to Town information may also be addressed under the *Municipal Conduct Act* and the Town's Code of Conduct. The CAO/Town Clerk and Town Council are responsible for ensuring that any appropriate technical and administrative safeguards are in place, as outlined in the *Towns and Local Service Districts Act*.

9. POLICY REVIEW

This policy is subject to review and modification as necessary to ensure it remains compliant with current legal standards and aligned with the overall mission of the Town of Pouch Cove. Violations of this policy may be subject to corrective action. This policy will be reviewed and updated annually and may be amended as required at any time between scheduled reviews.

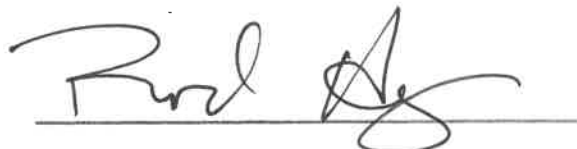
10. AMENDMENTS

11. EFFECTIVE DATE/RESOLUTION

This policy shall take full and immediate effect as of Aug 24, 2026.



Mayor
Brad Richards



CAO
Rodney Hynes

Aug 24, 2026
Date

August + 24/26
Date