



TOWN OF SLAVE LAKE
INFORMATION TECHNOLOGY POLICY

Directorate	Corporate Services		
Department:	Information Technology	Policy No:	CRS.IT-23.1001
Policy Title:	Mobile Client Computing Technology	Issue Date:	
Issued to:	All Employees	Policy Type:	New

Policy Statement

1. The Town of Slave Lake provides various mobile client computing technology, such as cell phones, smartphones, tablets, laptop computers, and mobile internet sticks (referred to as 'Town Mobile Devices') to elected officials, employees, volunteers, and other individuals ('Users') for conducting Town business. Department Directors are responsible for authorizing the issuance of these devices in accordance with this policy. Users are required to adhere to all applicable federal and provincial laws, the specific conditions outlined in this Policy, and all other Town policies that apply.

Purpose

2. This policy serves the following purposes:
 - a) To set forth the responsibilities and operational expectations for Users utilizing Town Mobile Devices.
 - b) To outline the requirements and duties related to the procurement, utilization, standardization, management, and disposal of Town Mobile Devices.
 - c) To establish rules and guidelines governing the permissible uses of TOWN Mobile Devices within the Town premises and to ensure appropriate and responsible utilization of this technology.

Scope

3. This policy governs the use of Town Mobile Devices, regardless of ownership (whether owned, leased, or licensed by the Town of Slave Lake) and applies to these devices regardless of their physical location.

Exclusions

4. The Chief Administrative Officer holds the authority to grant exemptions to this policy, either as standing exceptions or for specific instances, given the presence of a valid business reason.

Policy

5. Definitions

(a) In this policy, the following definitions apply:

- I. Mobile Client Computing Technology:** This encompasses cell phones, smartphones, laptop computers, tablet computers, mobile internet sticks, along with their respective usage plans and related peripherals.
- II. Usage Plans:** Refers to voice, text, or data plans, or any combination thereof, provided as a service by wireless carriers such as Bell, TELUS, or Rogers. Full functionality of cell phones, smartphones, and mobile internet sticks relies on appropriate usage plans. Additionally, laptops and tablet computers with built-in cellular data modems require usage plans for cellular wireless connectivity.
- III. Cell Phone:** A mobile telephone with built-in access to a cellular network, providing voice and texting capabilities, and sometimes equipped with camera and personal digital assistant features.
- IV. Smartphone:** A mobile phone that provides voice, text, email, calendar, internet browsing, and the ability to run applications.
- V. V. Mobile Internet Stick:** A USB device with a built-in cellular data modem, offering internet access (via a wireless carrier and data plan) to any TOWN Mobile Device it connects to.
- VI. VI. Laptop Computer:** A portable computing device with a built-in display, keyboard, and pointing device, typically featuring Wi-Fi capability, and optionally, cellular data connectivity for internet access through a wireless carrier.

VII. VII. Tablet Computer: A computing device accepting touch-based input directly to an LCD screen, eliminating the need for a mouse or keyboard (though detachable keyboard/mouse options may exist). It includes Wi-Fi capability and may offer cellular data connectivity for internet access through a wireless carrier.

VIII. Primary Compute Device: A desktop, laptop, or tablet computing device with sufficient performance to run the TOWN's standard operating system and most software applications used by the TOWN. It may serve as the sole compute device for certain TOWN employees.

IX. IX. Town Client Technology Standard: A Town document referenced in this policy, listing all TOWN approved client hardware devices and accessories.

6. Roles and Responsibilities

a) Information Technology

I. The Information Technology department is responsible for establishing and upholding corporate standards concerning Town Mobile Devices and their associated usage plans.

II. They provide support for Town Mobile Device hardware and software, ensuring smooth operations and troubleshooting as needed.

III. Budgeting all renewal costs for Town Mobile Devices falls under their purview.

IV. They handle the procurement process for Town Mobile Devices and their corresponding usage plans.

V. Maintaining an accurate inventory of leased or Town-owned mobile devices is part of their responsibilities.

VI. Regular reviews of Town Mobile Device use are conducted by the Information Technology department to assess performance and compliance.

VII. Arranging training sessions for Town Mobile Device Users is undertaken to ensure proficient and effective utilization of the devices.

b) Directors

- I. Directors or their authorized delegates are responsible for approving Town Mobile Device requests in alignment with this policy.
- II. They ensure that individuals issued a Town Mobile Device are well-informed about and adhere to this Policy.
- III. Budgeting and managing all costs related to the initial acquisition of Town Mobile Devices within their respective departments is part of their role.
- IV. Identifying personal use charges within their department that should be reimbursed to the Town is also among their responsibilities.
- V. Directors or their delegates are responsible for approving roaming plans or equivalent for Users traveling abroad, who require the use of a Town Mobile Device for work-related purposes.

c) Managers/Directors and/or Human Resources

- I. responsible for collecting Town Mobile Devices from Users at the end of their tenure and forwarding these devices to the Information Technology department.
- II. They ensure that Information Technology is informed, with sufficient notice, about Town Mobile Device requirements for new Users.

d) Users with Town-issued Mobile Devices

- I. Users must read, understand, and adhere to the Town Mobile Device Policy (this policy) and other relevant Town policies, including XXXX - Acceptable Use of Information Technology.
- II. Users are expected to attend and actively participate in training sessions for Town Mobile Devices when provided.
- III. Users are responsible for ensuring the protection of Town Mobile Devices against loss, harm, or theft. If the loss of these devices occurs as a result of user carelessness or disregard, the user will be held financially responsible for the complete cost of the device. Should an assigned device be lost or damaged, users are required to immediately notify the Information Technology department.

IV. Upon resignation, termination of employment, or at any time upon request, Users must surrender their equipment and related peripherals for inspection. Additionally, they are required to provide their device PIN/PW and deactivate any personal charge accounts associated with the device (e.g., Apple accounts). Failure to return the equipment in good working condition within a reasonable time frame (i.e., 24 hours) may result in the User bearing the cost of replacement. Outstanding debts for equipment loss or unauthorized charges may lead to the User being regarded as having left on unsatisfactory terms and subject to legal action for recovery of the loss.

7. Prohibitions

(a) n/a

8. Procedures and Guidelines

a) General

- I. Town Mobile Devices that have sustained damage and will not be replaced must be promptly reported to the Department Manager and Information Technology. Subsequently, mobility plans will be discontinued, and mobile capabilities for these devices will be deactivated.
- II. Town Mobile Devices that remain unused for an extended period exceeding one month should be reported to the Department Manager and Information Technology. As a result, these devices will be transferred to a minimum use plan.
- III. In the event of any User with a TOWN Mobile Device being on leave, excluding vacation, the device must be returned to Information Technology for temporary reallocation.
- IV. Lost or stolen Town Mobile Devices must be immediately reported to the Department Manager and Information Technology. If the device is stolen, individuals should promptly report the incident to the local police.
- V. The Town may conduct periodic audits of TOWN Mobile Devices, including evaluating their usage.

9.

b) Issuance of Mobile Client Technology

- I. The type(s) of Town Mobile Devices provided will vary based on individual needs, considering factors such as specific application or software requirements, working conditions, and mobility needs.
- II. The Town Client Technology Standard (Policy no. XXXX) establishes detailed criteria for device issuance, acting as a guide to determine the most suitable device for everyone. Eligibility for receiving Town Mobile Devices will be determined according to the conditions outlined in the Town Client Technology Standard.

c) Freedom of Information and Protection of Privacy

- I. Under the Freedom of Information and Protection of Privacy Act (FOIP), activity records for Town Mobile Devices, including but not limited to individual calls, emails, text messages, pictures, videos, and internet access history, are subject to potential release to the public.

d) General Acceptable Use

- I. Users who are provided with Town Mobile Devices must utilize these devices in strict adherence to the established IT acceptable use criteria, as outlined in Policy XXXX – Acceptable Use of Information Technology

e) Acceptable Personal Use

- I. Personal use of Town Mobile Devices must comply with all applicable conditions specified in Policy XXXX - Acceptable Use of Information Technology. Additionally, the following conditions pertain to the personal use of Town Mobile Devices:
 - Department Managers will review monthly invoices for their respective departments and inform Users about any additional personal use charges incurred. Users may be required to reimburse the Town for overages or additional charges resulting from personal use, as directed by their Department Manager.
 - Users are responsible for backing up any personal information (e.g., photos, videos, contacts) stored on Town-issued mobile devices.

The Town will not be held accountable for any loss of such information.

- Users must ensure that any non-Town standard media, software, or content installed or used on Town-owned devices complies with relevant terms, conditions, and licensing agreements.
- Records arising from the personal use of Town-issued mobile devices are subject to potential release to the public under the Freedom of Information and Protection of Privacy Act (FOIP).

f) Use of Town Mobile Devices While Operating Motor Vehicles

- I. With the exception of fire response unit and police services vehicles under the Traffic Safety Act exempted under the Motor Vehicle Act Town Representatives are prohibited from using Town Mobile Devices while operating a motor vehicle or motorized equipment. If a User is operating a vehicle, they should safely move out of traffic flow to the side of the road, put the vehicle into park and turn off the engine, before using their mobile device
- II. Users whose responsibilities include driving or equipment operation should refrain from using Town Mobile Devices while driving a vehicle or while driving any other vehicle (borrowed or their own vehicle) while conducting Town business. Drivers shall comply with all federal, provincial, and local laws and regulations regarding the use of mobile devices including cell phones. Incoming or outgoing cellular phone calls are not allowed while driving. Sending or reading text messages, emails, dialing cellular phones, viewing television, videos, or DVD's and inputting data into laptop computers, personal digital assistants or navigation systems are prohibited while driving. The cellular phone voicemail feature should be on to store incoming calls while driving and all message retrievals and calls should be made after the vehicle is safely parked.
- III. Hands Free Exception – In situations where responsibilities include regular driving and acceptance of business calls, hands-free equipment may be provided by the Town or an individual. Special care should be taken in situations where there is traffic, inclement weather, or individuals are driving in unfamiliar areas. Under no circumstances are Users required to place themselves at risk to fulfill

business needs. Additionally, all the following conditions must be met:

- The device is not held in their hand;
- The device is secured in the vehicle in such a way that it does not obstruct the operators vision or impede the operation of the vehicle;
- The device is configured with a hands-free accessory that is operated by voice recognition or activated by pressing a single button once to initiate or accept communication;
- If the hands-free device is a headset or earpiece, the headset or earpiece must be in place prior to operation of the vehicle and may be attached to one ear only – not both.

g) Travel and Roaming

- I. Using Town Mobile Devices for sending and receiving texts, emails, making calls, or utilizing data (e.g., internet use or applications that require internet connectivity) while abroad will result in additional costs for the Town. Users are accountable for consulting IT to understand the applicable rates for voice and data usage while outside of AB and Canada, and they must obtain approval from their managers before using Town Mobile Devices outside these regions. The following additional conditions apply to the use of Town Mobile Devices outside of AB and Canada:
 - The Town will cover the expenses for a temporary roaming plan or equivalent if travel outside Canada is deemed necessary for work, and the User needs to remain in contact while away. Similarly, if Users are traveling outside of Canada for personal reasons, but their responsibilities necessitate them to maintain close contact with the Town, a temporary roaming plan or equivalent will be covered.
 - Users are responsible for requesting a roaming plan or equivalent from Information Technology before their departure. In case of non-work-related travel outside of Canada, Users may request a roaming plan or equivalent, but they will be responsible for reimbursing the Town at the discretion of their manager or Supervisor.
 - Approval of roaming plans or equivalent is the responsibility of Department Directors or their delegates.

- Users must manage their device usage while abroad to avoid incurring excessive roaming fees. If excess roaming fees are incurred and are not the result of the employee conducting TOWN business, the User is responsible for reimbursing those charges at the discretion of their manager or Supervisor.

h) Cellular Data Consumption

I. While connected to any cellular network, Users must exercise caution with data-intensive activities, especially for personal use, when using Town Mobile Devices. Town Mobile Devices collectively contribute to a shared data pool, from which all devices draw data. Excessive data usage may deplete this pool, resulting in overage charges. Examples of data-intensive activities that Users should avoid while using Town Mobile Devices for personal use and connected to cellular networks include:

- Streaming Video (e.g., watching a one-hour high-definition YouTube video can consume upwards of 3GB of data).
- Visiting websites with embedded 'autoplay' video or audio (e.g., Facebook or Twitter).
- Video Chat.
- Streaming Music.
- Playing "Online" Games.

II. Town-issued mobile phones may be equipped with a 'Data Usage' app, designed to monitor cellular data consumption against monthly billing cycles. Users are encouraged to use this app regularly to keep track of their data usage and receive alerts if they approach or exceed monthly limits.

i) Wi-Fi Data Consumption

I. Most Town facilities have Town managed corporate Wi-Fi which allows Town devices to have connectivity to the internet without consuming data from the cellular network. Users should ensure Town Mobile Devices are connected to the Town's managed corporate Wi-Fi wherever possible as opposed to the cellular network.

II. Users may connect Town Mobile Devices to their home Wi-Fi network and engage in data-intensive activities provided they do

so under the conditions listed in this and other Town policies as they apply.

j) Acceptable Wi-Fi Networks

I. Users are permitted to configure Town Mobile Devices to connect with the following Wi-Fi networks:

- Town Corporate Wi-Fi
- Home Wi-Fi (provided it is password protected)
- Government-owned Wi-Fi (Federal, Provincial, Municipal)
- Wi-Fi owned and managed by reputable educational institutes.
- Free public Wi-Fi provided by reputable ISPs, including Shaw, TELUS, Rogers, and Bell

II. Users may configure Town Mobile Devices to connect with the above Wi-Fi networks. However, this should be kept to a minimum and only utilized when no other acceptable Wi-Fi networks are available.

Additionally, Users may configure TOWN Mobile Devices to connect with the following Wi-Fi networks:

- Hotel Wi-Fi
- Conference Wi-Fi
- Airport Wi-Fi

III. However, Users are prohibited from configuring Town Mobile Devices to connect with the following Wi-Fi networks:

- Unknown Wi-Fi networks
- Privately owned networks, including but not limited to coffee shops, restaurants, and book shops
- Tethering to Wi-Fi mobile hotspots through non-TOWN owned devices.

k) Tethering

I. When utilizing a Town Mobile Device to create a Wi-Fi hotspot, Users are accountable for ensuring that the device they are connecting is either a Town-owned device or a trusted personal device. Tethering is allowed only in situations where no other acceptable options are available.

I) Location Tracking

I. The Town will refrain from using location tracking on any client TOWN Mobile Device for the purpose of tracking Users or monitoring performance. However, mobile tracking capabilities may be employed under the following circumstances:

- During an Emergency Operations Center (EOC) activation, if a Town Mobile Device is issued to a User assigned responsibilities in this scenario.
- In the event of a lost or stolen Town Mobile Device.
- When tracking of a Town Mobile Device is required by law to support a legal investigation.
- If the User to whom the Town Mobile Device is issued specifically requests that location tracking be activated.
- In the context of purchasing and installing apps for personal use.

II. Users are permitted to purchase and install apps on Town-issued iPhone devices for personal use, if they adhere to the conditions outlined in this and other relevant Town policies. However, Town IT reserves the right to request the removal (uninstallation) of personal use apps from Town-issued iPhones if they are deemed to pose a risk to the Town. In such cases, Users must comply with IT's directives and promptly remove the apps.

Furthermore, Users are not allowed to purchase or install personal use (or business use) apps on any other type of Town Issued Computing Device, including laptop, tablet, and desktop computers.

II. Personal use apps for Town-issued iPhone devices should be purchased and installed using the Users' personal Apple ID.

III. Personal use apps for Town-issued iPhone devices may only be purchased from the official Apple App Store.

m) Purchasing and Installing Apps for Town Business

I. IT will handle the acquisition and installation of apps required for business use on all Town Mobile Devices. Requests for installing new business-related apps should be submitted to IT support.

m) Jailbreaking iPhone and iPad Devices

- I. Jailbreaking refers to altering the software on an iPhone or iPad device to remove restrictions imposed by Apple.
- II. Users must not jailbreak Town-issued iPhone or iPad devices under any circumstances.

o) Care and Protection of Mobile Devices

I. Mobile devices are susceptible to loss, theft, and damage. Users must exercise proper care for TOWN-issued mobile devices, which includes:

- Not leaving devices unattended in public places or visible within a vehicle, even if the vehicle is locked.
- Ensuring devices are securely stored in a cabinet, drawer, or office during non-working hours when left at work.
- Taking reasonable precautions to prevent physical damage, including using protective casing whenever possible.
- Avoiding use in inclement weather unless the device is equipped with a protective case.

p) BYOD – Bring Your Own Device

- I. Certain employees may find it necessary to utilize their personally owned mobile devices for official Town of Slave Lake business purposes. In such instances, the Town of Slave Lake has established a provision for a cellular allowance to be extended to employees who employ their personal mobile devices for work-related tasks. This allowance is subject to the subsequent stipulations:
 - Before utilizing their personal mobile devices for Town of Slave Lake business, employees must secure authorization from their respective director or manager. The authorization form, bearing signatures from both the employee's director/manager and the CAO, must then be submitted to the Finance Department.
 - Upon presenting an expense form along with a copy of the relevant invoice page from their cellular bill, employees are eligible to receive an allowance equivalent to either their monthly phone/data plan cost or \$40 per month, depending on whichever amount is lower.

It's essential to note that the Town of Slave Lake will not reimburse employees for any personal calls or messages made or received on approved personally owned cellular devices that are used for official company purposes.

q) Security and Device Management

- I. IT will enforce basic security measures on Town Mobile Devices, which may include device lock codes or passwords, auto-locking after a period of inactivity, account lock-out after failed login attempts, and drive encryption. Lock codes and passwords should not be shared.
- II. Smartphones and tablets owned by Users will only be allowed to connect to the Town's guest Wi-Fi network.
- III. Town Mobile Devices may be remotely wiped if:
 - 1) lost, stolen, or suspected of theft;
 - 2) the User's employment or tenure with the Town is terminated;
 - 3) a data breach, policy violation, virus, or similar threat impacting Town staff, infrastructure, or data is detected.

r) Environmental Sustainability

- I. Town Mobile Devices and other devices listed in the Town's Client Technology Standard will adhere to industry environmental and sustainability standards where possible.
- II. Town Mobile Devices will be disposed of in environmentally responsible ways, including reuse in economically challenged areas or non-profit groups and recycling according to provincial e-waste standards and guidelines.

s) Cost and Lifecycle Replacement

- I. Monthly usage costs, including voice, text, or data overages, will be paid by the User's associated business unit.
- II. Smartphone devices have no standard service duration and should remain in service if they meet business needs, are safe, functional, and provide adequate performance.

- III. The initial purchase cost of Town Mobile Devices and accessories should be budgeted by the User's associated department.
- IV. Replacement of Town Mobile Devices and accessories should be budgeted within the IT department budget.
- V. Managers in business units or service groups will decide when a device should be replaced or upgraded based on business needs.

t) Support

- I. IT is responsible for providing support for Town Mobile Devices, including repairs, upgrades, replacements, setup, troubleshooting, unpacking, and repacking.
- II. iPhone Users are responsible for OS upgrades as prompted by the device.

u) Loaner Pool

- I. In case of a Town Mobile Device failure, IT will maintain a pool of spare devices on a need basis subject to availability.


v) Violations

- I. Any violation of this policy may lead to disciplinary action (including suspension of privileges and/or device removal), dismissal, criminal charges, and/or legal action.

Related Policies

Other related policies include:

- (a) CRS.IT-23.1002 – Acceptable Use of Town Information Technology
- (b) CSR.IT-XX.XXXX - Town Client Technology Standards

ISSUED BY	APPROVED BY:	DATE:
1. Chief Administrative Officer		Sept. 15/23