POLICY 25-01	CELL PHONES

DATE OF ADOPTION:	June 24, 2025	**MOTION NUMBER:**	25/06/88
DATE OF AMENDMENT:		**DEPARTMENT:**	Corporate Services

PURPOSE

To establish the guidelines for the issuance, usage and reimbursement of Town of Vermilion Communication Devices as well as Personal Communication Devices utilized for conducting Town of Vermilion Business.

DEFINITIONS

Administration is the administrative Employees of the Town of Vermilion.

CAO is the Chief Administrative Officer for the Town of Vermilion.

Communication Device is a handheld device with the ability to receive and transmit voice, text, or data messages such as cell phones, smart phones, and/or blackberry's.

Director is a person employed by the Town of Vermilion who is in charge of an activity, department or organization, as delegated by the CAO.

Employee is an employee of the Town of Vermilion.

Manager is a person employed by the Town of Vermilion who is in charge of an activity, department or organization, as delegated by the CAO.

Personal Communication Device is a handheld device with the ability to receive and transmit voice, text, or data messages such as cell phones, smart phones, and/or blackberry' s owned and operated by an Employee of the Town of Vermilion.

Town is the Town of Vermilion in the Province of Alberta.

Town Business is professional services rendered for or on behalf of the Town of Vermilion.

SCOPE

This policy applies to All Members of Council and/or all Employees of the Town of Vermilion.

TASK	TITLE OR DEPARTMENT OF PERSON RESPONSIBLE
APPROVAL OF POLICY & AMENDMENTS	Council
HANDLING INQUIRIES & COMMUNICATING POLICY	Director of Corporate Services
MONITORING REVIEWS & IMPLEMENTATION	Chief Administrative Officer

GUIDING PRINCIPLES

- Administration is responsible for the purchase of Communication Devices for the purpose of conducting Town Business. All of the costs incurred in the purchase of Communication Devices is funded by the department by which it was approved.
- Communication Devices purchased by the Town are the property of the Town and must be returned to the Employee's Director when not in use or deactivated.
- The Town retains usage and call details for all Town owned Communication Devices. These records may be accessed by Town Employee's for audit and investigation purposes.
- Employees must read, acknowledge, and agree to in writing, Schedule A attached hereto, prior to being issued a Town owned Communication Device or receiving payment for their Personal Communication Device.
- The Town reserves the right to suspend the use of Town owned Communication Devices and withhold payment for Personal Communication Devices if an Employee is in breach of this policy.

ELIGIBILITY

- Employee eligibility under this policy is determined on a case-by-case basis. Written approval from the Employee's Director, or the CAO in the case of a Director, is required prior to an Employee being issued a Town owned Communication Device.

- Employees who have received written approval for the use of their Personal Communication Device receive a flat rate of sixty dollars ($60.00) per month.
- A Town owned Communication Device is provided to Employee's who participate in the Town's on-call rotation schedule.

ROLES & RESPONSIBILITIES

- Directors must:
    - Assess the Communication Device needs of their Employees to determine whether a Town owned Communication device should be issued or payment should be remitted for the use of their Personal Communication Device.
    - Ensure that inactive or unused Communication Devices have been returned and accounted for at the Town office.
    - Monitor the usage of Town owned Communication Devices to ensure compliance with this policy.
    - Notify the Director of Corporate Services of any Communication Device or plan changes.
    - Notify the Director of Corporate Services of any Communication Device reassignment.

- Employees must:
    - Abide by the terms and conditions of this policy with respect to their use of Communication Devices.
    - Use the Communication Device in accordance with the Town's Security Policy and Technology Access by Users Policy.
    - Immediately report a lost, stolen or damaged Communication Device to their Director.
    - Return any Town owned Communication Device including accessories to their Director at the conclusion of their employment.
    - Accept responsibility and fully reimburse the Town for the cost of replacing a Town owned Communication Device including accessories should it not be returned at the conclusion of the Employees employment with the Town.

SCHEDULE "A"

Bring Your Own Device (BYOD) User Agreement

This agreement outlines the terms and conditions for employees who choose to use personal devices for work-related purposes in the Town of Vermilion as per Policy 25-01, as amended from time to time.

Scope of Work-Related Activities

By signing this agreement, I acknowledge that "work-related activities" are included, but are not limited to:

- Accessing and responding to work email
- Participating in virtual meetings
- Accessing, editing, or sharing Town documents and files
- Using Town-approved collaboration platforms (e.g., Microsoft Teams, SharePoint, eScribe, CivicWeb)
- Logging into work systems (e.g., HRISMyway, and iCity Online)

Personal Responsibility and Cyber Liability

I acknowledge that I am personally responsible for the security, maintenance, and appropriate use of my personal device while used for work-related activities. I accept full liability for any data loss, unauthorized access, or cybercrime resulting from its use. I understand the Town of Vermilion is not responsible for damage, breaches, or losses involving my personal device.

Technical Security Requirements

I agree to implement the following security measures on any device used for work-related activities:

- BYOD monitoring (Miradore)
- Pin Code or biometric authentication (TouchID & FaceID)
- Auto-lock after inactivity (max 5 minutes)
- Regular operating system and security updates

Failure to meet these requirements may result in the revocation of BYOD privileges.

Initial _____

Organizational Access, Monitoring, and Remote Wipe

I acknowledge that the Town of Vermilion reserves the right to:

- Access or inspect work-related data on my device
- Request or perform deletion of such data as needed
- Remotely wipe work data in the event of loss, theft, policy breach, or upon termination of employment

I consent to these actions for the protection of Town data and systems.

Monitoring of BYOD devices may occur under the following circumstances:

- Upon initial approval of CAO
- In response to a security incident, policy violation, or legal requirement
- Upon termination of employment or BYOD agreement

Insurance

I agree to carry personal insurance sufficient to cover loss, damage, or liability related to the use of my personal device for work. The Town of Vermilion does not provide insurance for personal property.

Legal and Regulatory Compliance

I understand that any data processed on my personal device for work may be subject to applicable laws, including:

- Freedom of Information and Protection of Privacy Act (FOIP)
- Personal Information Protection Act (PIPA)
- Other relevant privacy/information laws in Alberta, Canada, or international jurisdictions where applicable

I agree that work-related data may be accessed, reviewed, or disclosed as required by law.

Personal Tax Implications

I understand that using my personal device for work and receiving a phone allowance may result in personal tax obligations under Canada Revenue Agency (CRA) guidelines. I accept full responsibility for consulting a tax professional and ensuring compliance with any applicable reporting requirements.

Initial _____

SCHEDULE "A"

Termination and Device Withdrawal

Upon employment termination or withdrawal from this agreement, I will:

- Remove all organizational data from my device within 30 days
- Grant access, if requested, to verify complete removal of Town data

Employee Name _____

Signature _____

Date _____

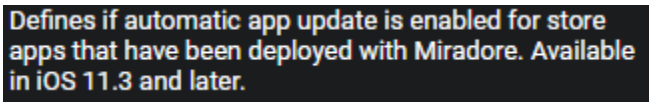
Miradore Business Policies

Bring Your own Device (BYOD) – Apple/Android

BP name:	BYOD Policy 2025
Tags:	• BYOD-IOS • BYOD-ANDROID
Configurations Profiles	• Auto-update apps • Location Tracking • Passcode settings • Restriction
Applications	• Outlook or Mail • Microsoft Teams • DUO Mobile • Miradore • Zoom (Optional) • Adobe (Optional)

Configuration Profile Details

Auto-update apps



Location Tracking

Minimum data update interval defines how often location updates are reported to the server.
Minimum distance change defines a threshold of how many meters the location of the device has to change before it receives location updates. Please note that when using small values, the device receives location updates more frequently and this shortens the battery life.

The above settings do not apply when Miradore client has been terminated, or the device has been rebooted, and the application is not running. In this scenario, the location of the device must change significantly before the client is launched by the iOS to report on the location.

Passcode Settings

Passcode settings	
Expiration age	6 months
Maximum screen lock timeout	Not set
History restriction	Not set
Require passcode to unlock (after)	Not set
Maximum number of failed attempts	Not set

Passcode requirements	
Allow simple value	☐
Require alphanumeric value	☐
Minimum length	4
Minimum number of complex characters	4

Restrictions

Security and privacy	
Deny personalized advertising from Apple	☐
Deny account modification	☐ S
Deny automatic updates to certificate trust settings	☐
Deny Bluetooth modification	☐ S
Deny USB restricted mode	☐ S
Deny device name modification	☐ S
Deny diagnostic data upload	☐
Deny diagnostic data setting modification	☐ S
Deny documents from managed sources in unmanaged destination	☐
Deny documents from unmanaged sources in managed destination	☐
Deny enterprise app trust	☐ S
Deny erase all content and settings	☑ S
Deny Files app network drive access	☐ S
Deny Find My Device	☐ S
Deny Find My Friends in the Find My app	☐ S
Deny Find My Friends setting modification	☐ S
Deny fingerprint unlock	☐
Deny notification modification	☐ S
Deny passcode modification	☐ S