The Corporation of the Town of Tecumseh

Policy Manual

Policy Number:	**115**
Effective Date:	**October 11, 2022**
Supersedes:	Not Applicable
Approval:	October 11, 2022
Subject:	**The Corporation of the Town of Tecumseh - BYOD Policy No. 115.docx**

Table of Contents

1.0 Purpose

1.1 The BYOD Policy (Policy) sets out the expectations and responsibilities of both the Town and Town personnel who use their own mobile device to access Town information assets.

1.2 Through this Policy, personnel will understand the requirements and responsibilities when using their own mobile device to access corporate information assets.

2.0 Scope

2.1 This Policy applies to all Town personnel and Elected Officials. Where third parties including contractors connect to the Town's networks using their own devices, the Policy will also apply.

3.0 Definitions

3.1 **BYOD** (Bring Your Own Device), for the purposes of this policy, refers to the devices owned by Town personnel and Elected Officials that are allowed to connect to Town networks and/or data for business purposes. These devices will be referred to throughout the policy as "personally owned devices".

3.2 **Corporation** means The Corporation of the Town of Tecumseh.

3.3 **Employee** means any person employed by the Corporation on a full time, part time, seasonal, student and/or casual basis. Also included are volunteers, contract workers, Council and Committee members who communicate with the public and/or represent the Corporation.

4.0 Policy

4.1 The Town recognizes that there may be a need or desire for Employees to only carry one mobile device with them while working. With a view to facilitating this, this policy has been developed to clearly define what is permitted and what is not when it comes to accessing corporate information assets with personally owned devices.

4.2 To access corporate information assets using a personally owned device, written approval must first be obtained from the head of the department that the employee works for.

4.3 Additionally, the personally owned device must be on the approved list created by the Town's Technology & Client Services (TCS) Department or approved by the Director TCS.

4.4 Employees and Elected Officials seeking to use their own device for Town-related business must make a request in writing using the appended form, which will also form the agreement with the Employee or Elected Official.

5.0 Permitted Devices

Subject to the make, model and operating system, the generally permitted devices include:

5.1 Smartphones

Acceptable smartphones are:

- Apple iPhones
- Samsung Galaxy
- Google Pixel

5.2 Tablet Computers

Acceptable tablet computers are:

- Apple iPad
- Samsung Galaxy
- Microsoft Surface

5.3 Non-Permitted Devices

Laptops, home desktop computers and, generally, devices that do not fall within the categories of smartphones or tablet computers are not permitted as personally owned devices able to connect to corporate information assets.

TCS have the right to deny or revoke the request if a permitted device or the operating system is not kept up to date.

6.0 Protection of Data on Personally Owned Devices

6.1 Passwords

All personally owned devices must be password or PIN protected. If using a password, the password must be:

- Unique – not a password used for other personal or business accounts
- Length – a minimum of 8 characters
- Complex – each password must contain at least:
    - One uppercase letter
    - One lowercase letter
    - One number
    - One special character (for example, @, #, $)

6.2 PINs

- If the device is capable of a 6-character PIN, this must be utilized
- Where the device is only capable of 4-character PINs, this is acceptable

6.3 Other

- Facial recognition
- Pattern recognition

6.4 Unattended Personally Owned Devices

Where possible, personally owned devices must be kept with the owner. When the devices are not with the owner, they must be automatically locked and protected with either a password or PIN as defined above.

6.5 Loss or Theft of Personally Owned Devices

If a personally owned device that has been approved to connect to corporate information assets is lost or stolen, it must be reported to TCS by the next business day.

If it is deemed necessary by the Town's TCS Department, employees should understand that the lost or stolen personally owned device may be remotely wiped clean to protect the Town's data. This may include the employee's personal data stored on that device. It is the responsibility of the employee to ensure that their personal data is backed up.

6.6 Monitoring of Personally Owned Devices

It is a requirement for all personally owned devices to be connected to the Town's network via the Town's Mobile Device Management (MDM) system.

While the Town will not actively monitor the activity of each device all employees should understand that this capability exists and may be initiated if deemed necessary. (ex. OS version up to date, location if lost or stolen, etc.)

6.7 Corporate and Personal Data

The Town's MDM will facilitate the separation of corporate and personal data on each personally owned device. This facilitates a level of protection of the Town's data and a level of privacy for the personal data on the personally owned device.

6.8 Encryption of Corporate Data

Encryption must be inherent in the approved device list. Confirmation of encryption capabilities will be determined by TCS Department upon request.

6.9 Confidential and Sensitive Data

Confidential and sensitive data must not be stored on personally owned devices. Types of data considered confidential or sensitive include, but are not limited to employee personal information, health information and personally identifiable information such as social insurance numbers. Town related data on personally owned devices constitute a 'Town record' and therefore are subject to search for any records, emails, etc. related to Freedom of Information requests to the Town.

6.10 Applications

The Town will not specifically prescribe which applications can and cannot be installed on personally owned devices. However, employees must not download or install applications that may affect the integrity of corporate applications and data. (ex. Virtual Private Network (VPN) software)

6.11 Cloud Technologies

It is not permitted to store any corporate data or information on cloud storage technologies unless explicitly approved by the Town. (ex. Dropbox, iCloud, OneDrive etc.)

6.12 Anti-Malware

The Town shall insist that a personally owned device must have anti-malware software installed on it. This is at the discretion of the Director Technology & Client Services.

7.0 Compensation and Costs

7.1 The Corporation will not reimburse employees for the use of their personally owned devices to access Town information assets and networks.

7.2 It is the responsibility of the employee to ensure that all costs associated with the personally owned device are borne and paid for by the employee,

including any costs associated with the upload or transfer of data or images related to work activities.

7.3 The Corporation is not responsible for any loss or damage to personally owned devices while being used for corporate business or personal activities.

8.0 Technical Support

8.1 Technical support from the Town's TCS Department will be limited to connectivity issues with the Town's networks and information assets, and associated corporate applications. The Corporation will not provide support on issues with personal connectivity or non-corporate applications.

9.0 Offboarding

9.1 Upon an employee leaving the Corporation, either voluntarily or at the discretion of the Town, the personally owned device will be wiped clean of all corporate data by the Town's TCS Department.

10.0 Responsibilities

10.1 All employees shall be responsible for following this Policy. This Policy will be reviewed as required based on revisions to corporate practices.

10.2 This policy will be posted on the Corporation's Intranet.

11.0 Termination of Access

11.1 As determined by the Director TCS or Designate, the Corporation retains the right to rescind access of any personally owned device if this Policy is violated or for any other reason that the Corporation considers meriting such action.

12.0 Related Documents

- Technology Acceptable Use Policy # 9
- Employee Code of Conduct

Appendix #1: BYOD Request & Agreement