


## The Rural Municipality of Elton

<b>REFERENCE:</b>	Personnel	<b>AUTHORITY:</b>	Council
<b>SUBJECT:</b>	The Use of Personal Devices and Security	<b>EFFECTIVE DATE:</b>	March 12, 2024
<b>ADOPTED BY RESOLUTION NO. &amp; DATE:</b>	2024-063 March 12, 2024	<b>NUMBER OF PAGES:</b>	3
<b>AMENDED BY RESOLUTION NO. &amp; DATE:</b>		<b>REEVE'S SIGNATURE FOR APPROVAL</b>	

### **PURPOSE:**

The purpose of this Policy is to establish guidelines for Council and Employees who choose to use their personal devices (such as smartphones, tablets, laptops, or computers) for the Rural Municipality of Elton (Elton) tasks. This Policy aims to ensure the security of Elton's data, maintain productivity and clarify the responsibilities of Council, Employees and Elton regarding the use of personal devices at work.

### **SCOPE:**

This Policy applies to all Council Members and Employees who wish to use their personal devices for municipal matters or work-related activities, regardless of their position within Elton.

### **SECURITY MEASURES:**

Council and Employees must implement and maintain the following security measures on the personally owned devices:

- All devices must be password protected.
- Devices must lock after five incorrect password attempts.
- Devices must time out and require a password after a five-minute (5) period of inactivity.
- Smartphones or Tablets that use Biometrics such as face recognition or fingerprint scans are acceptable supplementary forms of quick unlock, however these forms of quick access require a maximum six-digit (6) password upon restart of the device or biometric recognition failure.
- Computers and laptops must be password protected with a minimum complexity requirement of six (6) characters, a combination of upper and lower-case letters, numbers, and symbols.
- Computers and laptops must have Anti-Malware and Anti-Virus services installed.
- Council and Employees must immediately report any lost or stolen personal devices to the Chief Administrative Officer (CAO), if they have been used for Elton matters.

- In the event of a security breach or unauthorized access, Elton reserves the right to remotely wipe all Elton data and applications from personal devices.
- When upgrading a device, both the Council and employees are required to reach out to Elton's IT Service Provider to ensure that all data has been securely wiped from the previous device.

#### **SUPPORT AND MAINTENANCE:**

Council and Employees are responsible for the maintenance and upkeep of their personal devices. Elton's IT Service Provider will provide limited support for Elton related issues on personal devices, but Council and Employees should not expect the same level of support as provided for Elton-owned devices. Elton is not responsible for repairing or replacing personally owned devices.

#### **COMPENSATION:**

Elton provides compensation for use of personal devices which includes the use of smartphones, tablets, computers, internet, and printing for Elton business as stated by Council resolution.

- Payments shall be made quarterly for the preceding quarter in the months of March, June, September, and December.

#### **COMPLIANCE:**

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Additionally, legal action may be taken in case of data breaches or unauthorized access resulting from non-compliance with this policy.

#### **TERMINATION OF EMPLOYMENT:**

Upon the termination of employment, employees must cooperate with Elton and Elton's IT Service Provider to ensure the removal of any Elton data and municipal applications from their personal devices.

#### **PERIODIC REVIEW:**

This policy will be reviewed periodically by Elton or Elton's IT Service Provider to adapt to changes in technology, security threats and Elton needs. Employees will be notified of any policy updates.

#### **ACKNOWLEDGEMENT:**

By using personal devices for Elton-related tasks, Council and Employees must acknowledge that they have read, understood, and agreed to comply with this policy. Council and employees must sign the Policy declaration and have it placed in their file.



## DECLARATION OF THE USE OF PERSONAL DEVICES AND SECURITY POLICY NO. 89-2024

**Position:**

**Councillor**

**Employee**

I certify and attest that:

- I have read and understand the Rural Municipality of Elton's (Elton) Use of Personal Devices and Security Policy No. 89-2024
- I will abide by the guidelines set out by Elton.
- I understand that if any changes are made to this policy, I will be provided notice of the changes, and I will be required to sign a new declaration.
- I understand failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Additionally, legal action may be taken in case of data breaches or unauthorized access resulting from non-compliance with this policy.
- I understand upon the termination of employment, employees are required to cooperate with the Elton and Elton's IT Service Provider to ensure the removal of any Elton data and applications from their personal devices.

**Name:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Date:** \_\_\_\_\_

### OFFICE USE ONLY

- CAO filed in respective personnel file.

**Signature:** \_\_\_\_\_ **Date Received:** \_\_\_\_\_