CELL PHONE USAGE AND HANDLING

1. GENERAL

A. This policy outlines the guidelines for the usage and handling of cell phones issued to civilian and sworn employees. The purpose of this policy is to ensure that members effectively utilize these devices while maintaining the security and integrity of sensitive information.

2. POLICY

B. All members who are provided with a HRP issued mobile device shall ensure their usage is appropriate and consistent with HRP policy including security, privacy, and professional conduct.

C. Use of an issued device is a privilege granted by HRP and may be revoked at any time. The mobile device shall not be used for transmitting, retrieving, displaying or storing any information or images that may bring HRP into disrepute or impair the mission of HRP and/or the ability of personnel to perform their duties.

D. A mobile device shall be surrendered upon the demand of the employee's immediate supervisor.

E. HRP reserves the right to disconnect devices or disable services without notification.

F. Members shall not travel outside Canada with any HRP-owned mobile device unless they have received permission from their respective Divisional Superintendent.

G. It is the responsibility of the employee to ensure their usage of the issued mobile device is allowed under the current mobile device's monthly usage plan and no additional charges will be incurred that are not work related.

H. Costs associated to unauthorized personal use (i.e. international phone calls, text messages, internet usage, etc.) will be the responsibility of the employee.

I. Members are required to have their issued phones in operational condition, ensuring a charged battery, and on their person during working hours at all times.

J. All city-owned cellular devices are subject to the HRM Mobility Policy. Inappropriate use may result in disciplinary action and loss of privileges.

K. All electronic records (including text messages) are to be written in a professional manner. Any business related electronic record may be subject to a disclosure order or a request made through the Freedom of Information and Protection of Privacy (FOIPOP) Act.

Confidentiality and Data Security

L. Members shall exercise caution to prevent the unauthorized access to or disclosure of sensitive information stored on their mobile device.

M. Cell phones should be protected with strong passwords or biometric authentication, and officers shall not share their access credentials with unauthorized individuals.

N. When an issued phone has been lost or damaged, the following procedure must be adhered to:

   i. If lost or damaged, the employee must immediately notify their supervisor, who in-turn will notify HRM IT so the phone can be de-activated.
   ii. The employee must submit a HRP99 – Equipment Repair, Replacement or New Issue Form.
   iii. The issuance of a replacement phone will be on a case-by-case basis and may not occur if the loss or damage was due to negligence.

O. Officers shall not download or install unauthorized applications or software on their issued cell phones.

Effective Date	October 12, 2023
Policy Owner	Superintendent, Patrol

By Order Of:

Don MacLean
Chief of Police