Mobile Device Usage Policy

Purpose:

The purpose of this policy is to ensure appropriate use of corporately issued wireless handheld devices, provided to employees and members of Council for business purposes, while enhancing user safety, limiting corporate liability, protecting Township property and managing costs.

Scope:

This Policy applies to any person who has been given access to the Township of North Huron Information Technology (IT) Networks or data through mobile technology.

This Policy applies to any person who has obtained approval to access Township of North Huron Information Technology (IT) Networks.

This policy is intended to cover cellular telephone, PDAs, Blackberry, two-way radios and all other forms of mobile communication devices.

Policy:

ROLES AND RESPONSIBILITIES

1. Organizational Protocol:
   a. Where deemed necessary for the effective performance of job duties, the Township may provide an employee and/or member of Council with a Mobile Device to use for business purposes. The Township may require certain positions be in possession of a Mobile Device for such purposes as health & safety, emergency management, or other Township mandated purposes.
   b. Usage of any Mobile Device to perform work outside of the User’s regular working hours must be approved by the User’s supervisor. Being issues a Mobile Device by the Township is not, in itself, an approval to work overtime hours.

2. Any person who has been issued a Mobile Device is responsible for:
   a. Reading, understanding and signing the required “Mobile Device Policy Acknowledgement Statement”;
   b. Reading and understanding all training material, including updates as provided;
   c. Manage voice/text/data usage and ensuring adherence to the Mobile Device Plan;
   d. Obtaining approval and request procedures (see Data Management & Roaming)
when travelling out of country with a Mobile Device;

e. Taking reasonable precautions to ensure devices are not lost, stolen or damaged.
f. Ensuring that any Mobile Device issued for the purpose of emergency management, is monitored appropriately. In the event that the employee/member of Council takes Mobile Device with them on vacation/extended absence that the User must ensure that:

   i. Any emergency communication is promptly responded to by the absent employee; or
   
   ii. A “call forward” function is placed on the Device for the period of absence; or
   
   iii. The Mobile Device is left in the care and control of an Alternate.

3. IT Staff is responsible for:

   a. Providing accurate, timely and available training material to Mobile Device users;
   
   b. Providing timely Mobile Device support;
   
   c. Wiping and/or locking lost, stolen or otherwise compromised Mobile Devices that have been reported to IT Staff;
   
   d. Providing advice on the purchase of Mobile Devices, associated accessories and assisting with the activation of mobile plans on new devices;
   
   e. Reviewing this policy with staff;
   
   f. Ensuring Mobile Device owners have signed the “Policy Acknowledgement Statement”.

OWNERSHIP, PRIVACY AND PERSONAL USAGE

1. This Policy permits certain reasonable and responsible personal usage of the Township’s Mobile Devices. All personal usage must adhere to this policy and all provisions included in the Township’s Code of Conduct Policy.

2. Users that have been issued a Township Mobile Device may configure their personal email accounts on the device, provided the following conditions are met:

   a. Configuration and administration of personal email accounts is not supported by IT Staff, nor will personal data be backed up and/or restored;
   
   b. In the event a Mobile Device must be wiped, all personal data may be lost;
   
   c. In the event an employee is terminated, all personal data will be wiped;
   
   d. Mobile Devices cannot be connected to personal computer equipment;
   
   e. Is considered to be “use at your own risk”.

3. Users that have been issued a Township Mobile Device agree to and accept that his or her access and/or connection to the Township of North Huron networks will be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. This monitoring is necessary in order to identify accounts which may have been compromised by external parties or users who are not complying with Township policies. By accepting a Mobile Device, the user is consenting to the monitoring referred to in this Policy.

4. Unless otherwise approved by the CAO, all Mobile Devices must be returned to the user’s immediate Manager on termination/resignation/retirement, during periods of short/long term disability, during any other extended period of absence from work, or if requested to do so.
5. Council members and employees that leave the employment of the Township of North Huron and would like to purchase the mobile device issued to them, must do so in compliance with corporate policies and obtain approval from their Department Head, the CAO and in consultation with IT staff. The value of the mobile device will be determined by IT staff and approved by the CAO.

6. Council members that have been issued an iPad or other mobile device, will at the end of the term, be offered the opportunity to purchase the device. The value of the mobile device will be determined by IT staff and approved by the CAO. Any Council iPad that is not purchased by the member will return to the corporate IT inventory and disposed of in accordance with corporate policy.

SECURITY

1. Password Protection
   All Mobile Devices that access the Township’s Network or is used to store Township data (including email) must meet the following conditions:
   a. Must be encrypted using a password that meets standard guidelines for security. These guidelines are:
      i. Unique to the system that the password is used with;
      ii. At least 6 characters long;
      iii. Contain one of each of the following: lowercase characters, uppercase characters, numbers and symbols;
      iv. Contain no personally identifiable information i.e. family member names, pet names, anniversaries etc.;
      v. Contain dictionary words or letter or number sequences;
      vi. Must be known only to the Mobile Device user;
   b. Mobile Devices will be locked after a predetermined number of attempts to enter a password.
   c. All Apple ID login and passwords are determined by IT Staff and must not be changed by the User.

2. Users must immediately notify their Department Head and IT Staff if the Mobile Device is lost, stolen or is believed to have had security compromised in any way.

3. Users are prohibited from “Jail Breaking”, “Rooting” or performing any other changes that disables or modifies the hardware and operating system restrictions inherent on the Mobile Device;

4. IT will trace and where necessary, remote wipe any Mobile Device that is lost, stolen or is found to be in non-compliance with this Policy;

5. Camera phones may not be used to record confidential or proprietary information or to photograph Township premises unless authorized by Management. Township Mobile Device users shall seek permission from any employee/individual before taking their photo.

DATA MANAGEMENT AND ROAMING

1. All Mobile Devices are to be setup with the Township’s standard voice and text/data (where deemed necessary) plan. The plan may change without notice, as approved by
Council.

2. Users are responsible for ensuring usage adheres to the limits of the Township’s plan.

3. Tethering or establishing a data ‘hot spot’ is only permitted in emergency situations. Users are responsible for ensuring usage adheres to the limits of the Township plan.

4. IT Staff will provide documentation on how to manage cellular data usage, upon request.

5. Users who wish to travel outside of Canada with a Township owned Mobile Device (roaming) must:
   a. Obtain authorization, in writing, from the CAO at least 10 business days prior to the travel date;
   b. Upon approval of the CAO, arrange a roaming package that is required for the travel location and timeframe;
   c. Due to the expensive costs associated with roaming, users must be extra vigilant in ensuring they do not exceed the plan limits, and will be responsible for reimbursing the Township for any overages.

SUPPORTED DEVICES

The Township of North Huron, through IT Staff, will maintain a list of cost-effective devices and service plans available for use.

SOFTWARE (APPS)

Users may install Apps on their Mobile Device, without the intervention of the Township/IT Staff, providing the following criteria are met:
   1. The App is not known to cause any unacceptable security risk, as determined by IT Staff;
   2. The App does not cause degradation in the performance of the Mobile Device, as determined by IT Staff;
   3. The App is installed from approved sources (i.e. Apple App Store, Google Play or similar).

SAFETY

1. The Township of North Huron strictly prohibits the use of Mobile Devices while operating Township of North Huron owned and operated vehicles and equipment, or while operating a vehicle on Township of North Huron business.

2. The use of hands-free mobile phones should be kept to a minimum when driving. To make or receive calls, emails, texts, etc.:
   a. Pull over and stop;
   b. Allow a passenger to operate the Mobile Device;
   c. Use Voice Mail and respond at a safer time; or
   d. Let someone else drive, freeing you up to make or receive calls, emails, texts, etc.

3. Users are solely responsible for any fines and/or charges laid by the authorities for illegal use of a Mobile Device while operating a vehicle or equipment in the course of their employment. Users who choose to violate the policy will face disciplinary measures up to termination, or face legal responsibility if in the course and scope of their duties they are involved in a car accident and there is evidence that they were using the Mobile Device
while driving, and the Township of North Huron is sued.

**REIMBURSEMENT OF COSTS**

1. At the discretion of the CAO and in conjunction with the Finance Department, failure to properly monitor and manage voice, text and/or data usage, may result in the user being financially responsible for covering costs above and beyond the Township’s standard Mobile Device plan costs;
2. Users may be personally responsible for replacing lost, stolen or damaged Mobile Devices, if reasonable care was not exercised;
3. The Township reserves the right to collect the reimbursement of costs through standard invoicing and collection/and or payroll deductions;

**CONFIDENTIALITY**

1. The Township of North Huron is legally required to abide by certain confidentiality requirements and access procedures relating to records in the municipality’s custody or under its control. The requirements and procedures are set out in the *Municipal Freedom of Information and Protection of Privacy Act*. The records to which the Act relates include all materials stored on Township and/or other maintained systems. Users shall take all reasonable precautions to ensure compliance with the Act.
2. Before disclosing sensitive, confidential or proprietary information to third parties, by any means, employees must seek authorization from their Department Head.

**COMPLIANCE**

1. Users who have been issued a North Huron Mobile Device, must comply with the guidelines contained within the Mobile Device Usage Policy and acknowledge receipt and understanding of the said Policy by endorsement of the Policy Acknowledgement Statement.
2. Failure to comply with the Township’s Mobile Device Usage Policy may lead to legal, punitive or corrective action, up to and including termination of employment and/or criminal prosecution.
TOWNSHIP OF NORTH HURON
MOBILE DEVICE POLICY ACKNOWLEDGEMENT STATEMENT

I have read and understand the Township of North Huron Mobile Device Policy, including the limitations, conditions for personal use, and I agree and accept that the Corporation of the Township of North Huron has the authority to:

1. Monitor connections to the Township’s networks to record dates, times, duration of access etc. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including additional monitoring capabilities, eg. tracking application presence or usage, jailbreak detection, data usage, operating system version, may also be monitored;
2. Wipe the device remotely if it is lost or stolen, or if the employee leaves the organization. In the course of this action, I understand that everything is removed from the device including all corporate and personal data, including email, contacts, calendar appointments, personal pictures, network connections, etc.

EMPLOYEE NAME: ____________________________________________

DEPARTMENT: ________________________________________________

EMPLOYEE SIGNATURE: _______________________________________

DATE: ______________________________________________________

WITNESS SIGNATURE: ________________________________________