TOWN OF HINTON

POLICY TITLE:	Mobile Device/Bring Your Own Device Usage Policy
POLICY #:	097
EFFECTIVE DATE:	June 17, 2014
ADOPTED BY COUNCIL ON:	**June 17, 2014**

POLICY STATEMENT

Mobile devices are used to conduct Town business and enhance the effectiveness of communications with residents, colleagues, government and business. The Town network is a finite resource, which must be used responsibly to maintain its integrity and effectiveness and security.

1) PURPOSE

a) The purpose of this policy is to set the standards for the issuance, administration, use, and security of mobile information technology (IT) devices (Town or personally owned) that are used to conduct Town business, access or store Town information. These standards are established to protect the Town information on mobile IT devices, which consist of any non-stationary electronic apparatus with capabilities of recording, storing, and/or transmitting data, voice, video, or photo images and include laptops, personal digital assistants (PDAs), cellular phones, digital tablets, and any related storage media or peripheral devices.

b) Many employees carry personal devices in addition to the Town-issued devices. With the advances in technology, efficiencies can be gained through the combination of these devices.

c) This policy is linked to the Town's Electronic Network Policy and must be followed by all Town employees, councilors, contract personnel, volunteers and trainees;

2) DEFINITIONS/STANDARDS

a) "Mobile Devices" include but are not limited to personal and Town issued notebook computers, Windows and MAC laptops, tablets, cell phones, smart phones (e.g. BlackBerry, iPhone, Android, Windows), air cards, push to talk radios and modems. Device model and operating system version are approved at IT discretion.

b) "Users" include but are not limited to Town employees, council members, vendors, contractors, consultants and any other individuals with authorized access to and use of the Town's corporate networks, data and systems.

c) "Town Issued Devices" are smartphones, tablets and laptops purchased and provided by the Town of Hinton IT Department.

d) "BYOD" means Bring Your Own Device.

2.1) Scope

a) This policy governs the use of, and payment for, mobile devices required for business purposes. This policy applies when a director determines that an employee holds a position that requires the employee to be available to respond to business-related communication via phone, email, text, etc.

2.2) Exceptions

a) This policy does not apply to members of the Hinton RCMP.

2.3) Mobile Device Limitation

a) The organization allows up to two (2) personal devices for Town computing resources access for each participating user based on business need as approved by the director.

2.4) Personal Mobile Device

a) Employees may wish to use their own personal mobile device for work purposes as an alternative to being issued a Town device. Directors may provide the employee a monthly allowance of up to $35 as an offset for the business use of their personally owned mobile device. In the case of a monthly mobile allowance, the employee must sign the Mobile Device Agreement to be retained by IT as well as a signed copy of the Electronic Network Policy.

3) RESPONSIBILITIES

3.1) Directors

a) Make employees aware of this policy;

b) Determine if a position requires that the employee be regularly available to respond to business-related communication via phone, email, text, etc. in order for an employee to receive a TOH issued device, or a monthly mobile allowance for business use of a personal mobile device; and

c) Take appropriate action with respect to any breach of this policy.

3.2) Users of Town owned devices and personally owned devices

a) Agree to a general code of conduct that recognizes the need to protect confidential data that is stored on or accessed when using a mobile device.

b) Adhere to all applicable Town policies and laws to conduct Town business

c) Configure their mobile devices that are used to conduct Town business in such a way as to protect Town information.

d) Responsible for contacting the IT Help Desk immediately in the event that their Mobile Device is lost, stolen or if they have replaced their Mobile Device.

3.3) Users of personally owned devices

a) Responsible for, backing up all data, settings, media, applications, and installation of software updates/patches.

b) Responsible for all Mobile Device support requirements, including maintaining any necessary warranty information, battery replacement due to failure or loss of ability to hold a charge, and the cost of repairs or replacement.

c) Responsible for maintaining and paying the monthly/annual fee to the telephone mobile carrier. All mobile telephone charges that he or she incurs are his or her responsibility, regardless whether such charges are work related or for personal use. This includes, but is not limited to, charges resulting from texts, data plan surcharges, calls, navigation, or application uses or from early termination fees.

d) Submit an expense claim with the supporting documentation in order to be reimbursed for the use of their personal device.

3.4) Information Technology (IT)

a) Responsible for configuring and supporting the user's Mobile Device to access the Town's computing resources.

b) Will not offer support to personal devices other than initial setup of the device on Town systems and basic connection issues with the Town network.

c) Consult with the respective director or Town Manager any concerns they may have in regards to a User's misuse of Town devices before taking action to remove a user from the network or "remote wipe" the Town data on a Mobile Device.

d) Responsible for mobile device system removal and performing a "remote wipe" of Town data from a user's lost or stolen Mobile Device. In some situations, IT may perform a full device wipe after providing sufficient notice to the User to allow for personal data backup.

e) Responsible for mobile device system removal and performing a "remote wipe" of Town data from a user's Mobile Device upon termination of employment with the Town.

4) PRIVACY EXPECTATIONS

4.1) Town Issued Devices

a) Town employees have a right to a reasonable expectation of privacy while using Town provided devices. Employees, who wish that their private activities remain private, should avoid using the Town provided device for personal use. The Town can undertake monitoring beyond its ordinary network performance monitoring activities even with respect to information in which the authorized individuals have a reasonable expectation of privacy, as long as the monitoring is reasonable. That is, it must be (a) authorized by law; (b) the lawful authority must be reasonable; and (c) the search must be carried out in a reasonable manner.

4.2) Personally Owned Devices

a) The Town will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads town email/attachments/documents to their personal device).

b) The user must register their mobile device with IT.

c) The Town will install Mobile Device Management software and, as such, will have access to configuration information on the device including location, installed applications, data quantity and other device related information.

5) DATA SECURITY

5.1) Town Issued Devices

a) Town owned mobile devices are centrally managed by IT. The user is responsible for:

i) Exercising reasonable care to prevent abuse or theft;

ii) Contacting the IT Help Desk immediately in the event that their mobile device is lost, stolen or compromised;

iii) Adhering to the acceptable device and network use policy;

iv) Keeping passwords confidential.

b) The user will not backup, download or transfer sensitive business data/documents to any third party service.

5.2) Personally owned Devices

a) Device Reset and Data Deletion

i) The user understands and accepts that Town data on the device will be removed remotely under the following circumstances:

a) Device is lost, stolen or believed to be compromised;

b) Device is found to be non-compliant with this policy;

c) Device inspection is not granted in accordance with this policy;

d) Device belongs to a user that no longer has a working relationship with the Town;

e) 15 incorrect password attempts; or

f) The user decides to un-enroll from the program or access is no longer required.

b) Wi-Fi Access to Corporate Network

i) Users connecting to the Town Wi-Fi network with a personally owned device will be allowed access to corporate systems and resources available via the Internet and are subject to the Electronic Use Policy using their personally owned device while connected.

c) Rooted or jail broken phones will be removed from TOH network access.

d) The user will not backup, download or transfer sensitive business data/documents to any third party service.

6) TOWN OF HINTON'S RIGHT TO MONITOR AND PROTECT

6.1) The Town has the right to:

a) Monitor corporate messaging systems and data including corporate data residing on the user's mobile device;

b) Modify, including remote wipe or reset to factory default, the registered mobile device configuration remotely;

c) Monitor corporate messaging, review, disclose or access incoming and outgoing messages in the ordinary course of business at any time with or without notice.

d) If the user uses a personal mobile device for Town business and the Town determines that the confidentiality, integrity, and availability of Town information is at risk as a result of that use then IT in consultation with the respective director or Town Manager may take the following steps.

i) Remotely wipe all data from any device connected to the Town infrastructure, including personal information.

ii) Require the user to remove any Town-related business information from a personally owned or managed data repository.

iii) Provide unrestricted access to the device to access corporate data repositories and Town related content.

e) The Town may, without intention, access private information stored on the personal device.

7) PROCEDURES

7.1) Approval

a) Directors are responsible for determining which positions should be available to respond to business-related communication via phone, email, text, etc in order for an employee to receive a Town issued device, or an allowance for business use of a personal mobile device.

b) In the case of a mobile allowance, the employee must sign the Mobile Device Agreement to be retained by IT and sign a copy of the Electronic Network Usage Policy.

7.2) Enforcement

a) Any use of the Town's technology resources that breaches this policy will be considered misconduct and will be reviewed. This may result in follow-up action including a range of administrative and disciplinary options in accordance with the practices of the Town including but not limited to:

i) Account suspension;

ii) Revocation of device access to the Town's technology resources;

iii) Data removal from the device;

iv) Take administrative or disciplinary action even when a criminal charge or civil lawsuit is not pursued.

7.3) Terms of Device Replacement

a) Devices will be available for upgrade or replacement based on the plan renewal dates (a three year term); lost, stolen, damaged devices will be replaced at director's approval.

Bring Your Own Device User Acknowledgment and Agreement

It is the organizations right to restrict computing privileges, or take other administrative action due to failure to comply with the above referenced Policy and Rules of Behavior. Violation of these rules may be grounds for disciplinary action in accordance with the disciplinary practices of the Town of Hinton.

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my usage of Town services.

I understand that the Town is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device in this program.

I understand that business use may result in increases to my personal monthly service plan costs. The Town may contribute up to $35 towards my monthly costs however I am responsible for maintaining and paying all fees to my mobile carrier.

Should I later decide to discontinue my participation in the BYOD or cease to remain an employee or replace my Mobile Device, I will allow the Town IT staff to remove and disable any Town provided software and services from my personal device. This may require a factory reset/full wipe to be performed on my Mobile Device.

User Name: _____

User Position: _____

Approved Device(s): _____

_____

Employee Signature: _____Date: _____

Director Signature _____ Date: _____