



## 1. STATEMENT

Mobile handheld devices are tools that can help employees manage their job responsibilities while they are away from the office.

Mobile handheld device users must comply with government policy and legislative requirements for asset and records management, privacy, security, and acceptable use.

Only mobile handheld devices that are owned by the GNWT may access GNWT services and infrastructure (e-mail, PCs, and the network).

## 2. SCOPE

This policy applies to all GNWT Departments, Boards and Agencies that use government e-mail provisioned by the TSC through the GNWT's Microsoft Exchange® e-mail server. The term "Department" throughout this document shall also mean Board(s) and Agency(ies).

## 3. DEFINITIONS

Mobile handheld devices are used to send and receive voice, text, data, and/or email messages and are categorized as follows:

Cell phone – A cell phone is a mobile handheld device that allows a user to send and receive voice messages, Short Messaging Service (SMS or 'text') messages, take and send pictures, and access the Internet, via a cell-phone network.

Smartphone – A smartphone is a mobile handheld device that has the same functionality as a cell phone and includes the ability (among others) to send and receive e-mail messages, store information, and install programs. RIM BlackBerry® is the GNWT standard for smartphones that will be used for GNWT e-mail.

Personal Digital Assistant (PDA) – A PDA is a mobile handheld device that allows a user to manage contacts, appointments, tasks and other information. Users keep PDAs current by synchronizing the device with a desktop computer over a cabled or wireless connection.

Throughout this document, all of the above will be referred to as "mobile handheld device(s)".



## 4. ROLES and RESPONSIBILITIES

### The Informatics Policy Council (IPC)

- The Deputy Ministers' committee responsible for approving informatics policy.

### Departments

- Departments are responsible for determining who is eligible to have a mobile handheld device.
- The Deputy Minister (or designate) authorizes the purchase, and the Department is responsible for purchasing mobile handheld devices, and paying monthly service contract fees and TSC chargebacks (if applicable).
- Departments are also responsible for ensuring that users return mobile handheld devices when they are no longer required (Asset Management – refer to the “Supporting Documentation” section).

### Department Telecommunications Coordinator (TC)

- The TC is the person designated as the primary administrative contact for the Department's mobile handheld device users, the TSC, and Service Providers, regarding the Department's telecommunications services.
- TCs may purchase mobile handheld devices for authorized users as detailed in the procedures.
- TCs coordinate Departmental account inquiries, mobile handheld device service and change orders, and participate in reconciliation and billing/reporting activities.

### Users

- Users are employees approved to use a GNWT mobile handheld device.
- Users are responsible for device use and safekeeping and must be aware of, and comply with, applicable GNWT policies, procedures, standards, guidelines and best practices (refer to the “Supporting Documentation” section).
- Users must report loss, theft, damage or suspected misuse and/or device compromise as outlined in the procedures, and promptly return the mobile handheld device to the Department if it is no longer required.
- Users are not expected or required to respond to work-related messages received via their mobile handheld device outside of regular working hours unless their job description specifically includes after-hours or on-call responsibilities.

## **Technology Service Centre (TSC)**

- The TSC is responsible for IT infrastructure and network services.
- The TSC establishes mobile handheld device procedures covering authorization, acquisition, inventorying, security, use and disposal.
- The TSC provides mobile handheld device users with support including information about device use, security features and contact numbers for service.

## **The Office of the Chief Information Officer (OCIO)**

- The OCIO is responsible for corporate informatics policy development, interpretation and revision.

## **5. POLICY**

### **5.1 Eligibility**

Departments are responsible for determining users who are eligible for a mobile handheld device. Eligibility considerations include:

- Senior Management – who may be expected to respond to work-related messages beyond normal working hours;
- Subject matter experts – who may be required to provide immediate responses to Senior Management;
- Highly mobile employees – frequent travellers whose productivity can be maintained through use of a mobile handheld device;
- Front line personnel – who require a mobile handheld device to assist in delivering services directly to clients;
- Safety – personnel who require communications capabilities as they may be subject to health and safety risks;
- Critical systems support personnel – employees who need to be contacted to provide after-hours or crisis response support;
- Service coverage – mobile handheld devices may not work in all NWT communities.

## 5.2 Compliance

Users must comply with other GNWT legislation, policies, procedures, standards, and guidelines related to mobile handheld device use. Refer to the “Supporting Documentation” section of this policy for more information. Specific considerations include:

### 5.2. a) Government Records

- Users should be aware that information transmitted or received using a GNWT mobile handheld device is considered a government record and is subject to requests for information under the *Access to Information and Protection of Privacy Act* (ATIPP);
- An access to information request for cell phone voice or text messages requires authorized personnel to review all records held on the mobile handheld device. Users should be aware this may involve a review of personal messages in addition to work related messages;
- Users should also be aware that Section 47(1) of the ATIPP Act specifically states individual employees have a direct responsibility for the security of the personal information used within their performance of services for a public body.

### 5.2. b) Security

Where technically possible, the TSC pre-configures GNWT mobile handheld devices with security settings. This helps to manage risk should the mobile handheld device be lost or damaged and helps to ensure compliance with ATIPP legislation and GNWT policy on electronic information security and records management.

### 5.2. c) Limited Personal Use

The GNWT Code of Conduct and personal limited use provisions of the Internet Use Policy (#6003.10.10) and the Email Use Policy (#6003.10.11) apply to all mobile handheld device users.

### 5.2. d) Proper Use

- Do not use a GNWT mobile handheld device while driving unless a hands-free kit is used;
- Do not use a camera-equipped GNWT mobile handheld device to take pictures of people without their permission, or capture copyright protected, sensitive, or confidential documents;

- Do not leave mobile handheld devices in charging stations in the office overnight. Keep them secure if they're not with you;
- Do not check mobile handheld devices into your luggage when travelling. Keep the device with you at all times.

## 5.2. e) TSC Support for Standard and Non-Standard Mobile Handheld Devices

- Cell Phones: There are no GNWT cell phone standards. Users may select a cell phone model of their choice.
- Smartphones: RIM BlackBerry® is the GNWT standard for smartphones that require access to GNWT e-mail services. Users of these mobile handheld devices will be supported by the TSC and permitted to access GNWT e-mail services. Non-BlackBerry® smartphones will be blocked from accessing GNWT e-mail services.
- Personal BlackBerry® Devices: Personal (non-GNWT owned) BlackBerry® devices will be blocked from accessing GNWT e-mail services;
- PDAs: Storage of GNWT records (i.e. emails) on PDAs and access to calendaring functions is permitted, provided the device is secured to acceptable levels. This level must meet or exceed the security of a BlackBerry device.

## 5.3 Corporate Rate Agreement

The GNWT has corporate rate agreement(s) that Departments must use when purchasing service plans for cell phones, smartphones, and BlackBerry® devices. The TSC and Department Telecommunications Coordinators have information about available service plans and Department account numbers.

## 5.4 Chargebacks

Departments will be billed a monthly TSC chargeback fee for BlackBerry® users to cover licensing and TSC support costs.



**6. SUPPORTING DOCUMENTATION**

<i>Document Title</i>	<i>Reference</i>
Electronic Information Security Policy #6003.00.26	
Recorded Information Management Policy #6003.00.18	Section 3 (III) a-d, Section 6 (II) bullet4, Section 6 (IV)
Electronic Records Management Policy #6002.00.20	Section 3 (I), (II) b
Managing Electronic Mail Guidelines #6003.00.21	Items 1.3, 1.4, 2.2, 2.3, 2.4 and 2.5
Access to Information and Protection of Privacy Act	Sections 42, 47(1)
Loss of Cash or Other Assets	FAM, Section 4101 (formerly 913)
Internet Use Policy # 6003.10.10	All
Email Use Policy # 6003.10.11	All
Code of Conduct Respecting Conflict of Interest and Oath of Office and Secrecy (March 2008)	Section 76 and 77
Mobile Handheld Device Procedures	Posted on TSC web site

**7. IMPLEMENTATION**

This policy comes into effect immediately upon approval by the Informatics Policy Council.

  
Chair

Informatics Policy Council

November 7, 2008  
Approval Date