



COMMUNITY AND GOVERNMENT SERVICES

ACCEPTABLE USE OF HANDHELD WIRELESS DEVICES POLICY

PREAMBLE

The use of wireless technology now requires a policy to ensure Government of Nunavut (GN) Information is handled in compliance with current GN policies and legislation. The *Archives Act*, the *Access to Information and Privacy Act*, records management policies and information security procedures require that the actions and decisions taken by the public servants be properly recorded, documented and secured. When significant information is exchanged or decisions are made in the course of a meeting, telephone call, instant text messaging, or via e-mail, staff must ensure that a record of the exchange is properly stored and managed using GN facilities.

PRINCIPLES

- The GN provides handheld wireless devices to employees where it is necessary for the effective performance of an employee's duties. These services shall only be used in a manner which protects system resources and the information stored therein, and which is accountable and consistent with the provision of ethical, courteous and professional service to Nunavummiut.
- The GN has a statutory obligation to protect electronic records and to maintain the continuity of government services.
- The GN is committed to Inuit Qaujimajatuqangit principles of Piliriqatigiinni-
lkajuqtigiinni- (working together for a common cause) and Pilimmaksarniq-
Pijariuqsarniq (development of skills through practice, effort and action).
- In accordance with Pinasuaqtavut values, self-reliance will be advanced by supporting the integrity of the GNs network operations and ensuring that government records are retained in a secure environment.
- In accordance with Pinasuaqtavut values, this policy will be fair, easy to understand and encourage staff compliance and accountability.
- The GN has a statutory obligation to protect personal information by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of information and records under its control.
- The GN has a statutory obligation to ensure that the public has access to all government records, including electronic ones.

DEFINITIONS

“Handheld Device” includes any portable wireless, telephone, Email or Internet communications device.

APPLICATION

This Policy applies to all GN employees who use wireless devices for government business and to all applicable agencies and crown corporations.

Rules of use:

1. Departments shall procure wireless telecommunications devices only in accordance with the requirements of Chapter 1000 of the Financial Accounting Manual regarding purchasing of information technology and only where staff members have agreed to comply with all related policies, procedures and guidelines laid out for such equipment by the Department of Community and Government Services and Informatics Planning and Services.
2. Prior to purchase, departments must provide Informatics and Planning Services with specific device requirements and specifications and once received, IPS must manage all aspects of device configuration and installation related to the security of their device.
3. Personally owned wireless devices must not be connected directly within any GN network. They may only be used from outside the GN firewall.
4. All wireless devices and their communications are subject to the GN's *Email and Internet Acceptable Use Policy*.
5. Peer to peer networking of wireless devices is strictly forbidden.
6. Wireless devices are capable of operating in an “always on” mode and can be susceptible to outside attacks. This is compounded by the fact that information is retained within the device and on non-GN computer systems belonging to the Service Provider providing wireless access. GN users assigned one of these devices shall therefore be accountable for security and privacy due diligence regarding all GN data and communications created through the use of their assigned device.
7. The integrity of Government networks and system resources is critical to the provision of that public service and accordingly the Government automatically monitors their performance and reliability. Failure by a user to adhere to policies pertaining to a wireless device can expose the GN to risks and vulnerabilities which result in legal and financial liability

8. All GN wireless communications records shall be subject to all laws, policies and procedures that apply to the management of any other GN information or record. As per the *Archives Act* and the Records Management Policy every decision and communication with respect to GN related business must be documented and accessible for posterity and reference.
9. Users should be aware that authorized requests under *the Access to Information and Protection of Privacy Act*, the *Criminal Code of Canada*, or during the GN's maintenance and system administration routines required to ensure reliability, traffic flow, and to exercise due diligence against liability for misuse, may require the disclosure of the contents of any record created or recorded stemming from the use of a handheld wireless device, personal or otherwise, to appropriate authorities.
10. All records created on, or duplicated from, a handheld device issued by the GN, including back-up copies, are considered to be the property of the GN, not the property of the user.
11. Some non-business use of handheld devices is provided for in article 14 of the Collective Agreement. That use is also subject to this Policy.

ROLES AND RESPONSIBILITIES

The Minister

The Minister of CGS is accountable to Cabinet for the implementation of this policy.

Deputy Minister

The Deputy Minister of CGS:

- (a) is responsible for the administration of all provisions pursuant to this policy;
- (b) may through a letter of instruction, delegate authority to the Corporate Chief Information Officer as deemed appropriate by the Deputy Minister.

Deputy Ministers of each department have are responsible to ensure that their staff are aware of and required to adhere to this Policy.

Departments

Departments will be responsible for:

- classifying, scheduling, and managing their records to meet the operational and administrative needs of their programs, including the need to be accountable for program operations;
- managing of records to meet the public policy requirements set out in the *Financial Administration Act*, the *Archives Act*, the *Access to Information and Protection of Privacy Act*, and other acts, regulations and policies that may affect their specific programs and records;
- accessing the advice and expertise available in other departments with managing records in the context of public policy; and
- designating a responsible official to be the departmental liaison with Records Management and develop records schedules for operational requirements, and to deal with public policy issues that may arise with respect to their records.

PREROGATIVE OF CABINET

Nothing in this policy shall in any way be construed to limit the prerogative of Cabinet to make decisions or take action respecting E-Mail and internet services acceptable use policy.

SUNSET CLAUSE

This policy shall be in effect from the date of the signature until June 30, 2012.

Paul Okalik
Premier