



Policy

6003.10.11

*Informatics Policy Committee
E-mail Use*

Revisions Table

<i>Version</i>	<i>Author</i>	<i>Description</i>
Use of Electronic Mail and the Internet (Guidelines)	Information Management Section, FMBS	Approved: February 26, 2002 Rescinded: March 17, 2008
E-mail Use (Policy)	OCIO	V1: June 18, 2007
		V2: July 5, 2007
		V3: July 30, 2007
		V4: October 22, 2007
		V5: November 5, 2007
		V6: December 10, 2007
		V7: February 4, 2008
		V8: March 26, 2008 (final)

1. STATEMENT

E-mail services are provided to Government of the Northwest Territories (GNWT) employees for work-related activities and must be used and managed in a responsible manner and in accordance with related GNWT legislation, policies and standards.

2. PURPOSE

The purpose of this policy is to provide guidance on the use of GNWT e-mail, explain the impacts it can have on shared technology resources, and provide clarity on related security, privacy and records management matters.

This policy complements the Code of Conduct Respecting Conflict of Interest and Oath of Office and Secrecy for Employees of the Government of the Northwest Territories ("The Code of Conduct").

In this policy, the term "e-mail" includes electronic mail systems (e.g. via a computer, Webmail, or mobile e-mail), provided by the GNWT.

This policy applies to users in all Departments, Boards, Agencies and other organizations who have been granted access to any GNWT e-mail system.

3. AUTHORITIES (Roles and Responsibilities)

The Informatics Policy Committee (IPC), a committee of Deputy Ministers with responsibility for informatics policy for the GNWT including approval and review of this policy.

Deputy Heads are responsible for overseeing e-mail use within their respective departments and ensuring adherence to all related legislation, policies and standards.

Employees/Users are responsible for exercising reasonable judgement when using government e-mail so that their actions are not illegal, do not degrade the performance of shared technology resources or compromise their security, or cause incremental expense for the GNWT.

Managers/Supervisors are responsible for ensuring that employees follow approved records management procedures for e-mail messages and for initiating action regarding inappropriate e-mail use as per the Code of Conduct.

The Department of Public Works and Services (PWS), Technology Service Centre (TSC) is responsible for providing government e-mail services, and for monitoring and reporting on e-mail services and network use and performance.

The Department of Human Resources (HR) provides assistance with investigations and actions arising from employee behaviour that contravenes the Code of Conduct.

The Office of the Chief Information Officer (OCIO) is responsible for policy interpretation, revision and recommending policy changes to the IPC. The OCIO may also assist in investigations arising from this policy.

The Audit Bureau may be called upon to conduct investigative audits arising from this policy.

4. PRINCIPLES

1. **Appropriate Use** - E-mail access is provided to facilitate GNWT business communications; it can be used to provide timely and courteous service to the public.
2. **Privacy** - Network use, including e-mail activity, is monitored and regularly reported to Deputy Heads. Users should have no expectation of privacy regarding e-mail messages they create or receive using government resources. Information created using government computers, facilities, networks or resources (including e-mail) is considered a government record and can be accessed by the public under the Access to Information and Protection of Privacy Act (ATIPP).

(References: Access to Information and Protection of Privacy Act and: Standard of Best Practices for Information Security Management (6003.00.27), Section 5.0 Security Management – S.M. 5.3 Electronic Mail)

3. **Security** - Employees have an obligation to protect government information and the integrity of government assets, infrastructure and resources.

(References: Electronic Information Security Policy (6003.00.26); Management of Electronic Information Policy (6003.00.20); Recorded Information Management Policy (6003.00.18); Access to Information and Protection of Privacy (ATIPP) Act.)

4. **Personal Use** – Limited and occasional personal use is permitted under the Code of Conduct provided it does not negatively impact performance of work responsibilities. All employees are expected to use common sense and good judgement when using e-mail as they are responsible for e-mail sent using their sign on ID, and must ensure that their e-mail use does not negatively impact shared government resources or create incremental expense to the GNWT. Employees should seek further guidance from their Supervisor if they are uncertain regarding appropriate use.

In accordance with the Code of Conduct, the following activities are expressly forbidden:

- a) Conducting illegal activities.
- b) Sending messages and/or attachments that contain racist, sexist or sexually explicit items or content including: pictures, jokes, hoaxes, or executable graphics.
- c) Sending hate mail, harassing others, making discriminatory remarks, or using objectionable language.
- d) Misrepresenting other employees on any GNWT network by sending e-mail from another user's computer.
- e) Conducting or pursuing their own business interests or those of another organization.
- f) Political lobbying.

5. PROCEDURES

1. Employees are required to use the gov.nt.ca e-mail or other government address domain for all government communications, as e-mail messages are considered government records.
2. While occasional use of e-mail for personal reasons is permitted and described in the Code of Conduct, employees are encouraged to obtain and use personal e-mail accounts for personal business, as personal e-mail sent from a government email domain such as gov.nt.ca can be perceived by recipients to officially represent the GNWT.
3. Employees who receive personal e-mails to their government account are advised to re-direct the messages to a personal account and ask the sender to use the personal account in future. Decreasing the amount of non-work related messages can help employees stay within their allotted e-mail account quota and help the GNWT manage the network and storage requirements for e-mail.

4. The following e-mail activities are not allowed because they present either a security risk, can negatively impact shared technology resources and performance for all users, or have the potential to cause additional expense to the GNWT:
- a) Creating or distributing messages with large distribution lists or attachments. Employees are encouraged to use the GNWT's File Transfer Protocol (FTP) service for large file attachments, and collaboration tools available through Microsoft Office (Sharepoint) for document sharing when possible to minimize impacts on shared technology resources.
 - b) Downloading content from personal e-mail messages and storing them on GNWT computers (chain letters, junk mail, advertisements, executable graphics, personal photos, music). Storing these items on government computers can take up storage space on the network and create additional expense for the GNWT.
 - c) Divulging, sharing or compromising government authentication credentials with unauthorized users. (*Reference: Standard of Best Practices for Information Security Management (6003.00.27), Section 4.0 Information Processing – I.P 4.7 User Authentication*)
5. Employees who violate this policy may be subject to disciplinary action up to and including dismissal.

6. SUPPORTING DOCUMENTATION

Document References

Document Title	Reference
Access to Information and Protection of Privacy Act (ATIPP)	Section 2 - Definition of "record" (Pg. 9)
The Code of Conduct Respecting Conflict of Interest and Oath of Office and Secrecy for Employees of the GNWT	"Use of Government Equipment and Property" - Item 76 and 77
Recorded Information Management - Policy	IPC Policy #6003.00.18
Management of Electronic Information - Policy	IPC Policy #6003.00.20
GNWT Electronic Information Security - Policy	IPC Policy #6003.00.26



Policy

6003.10.11

*Informatics Policy Committee
E-mail Use*

Document References

<i>Document Title</i>	<i>Reference</i>
Electronic Information Security - Standards of Best Practice for Information Security Management	IPC Policy #6003.00.27 <ul style="list-style-type: none">• I.P. 4.7 User Authentication• S.M. 5.3 Electronic Mail

7. IMPLEMENTATION

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

This policy replaces the "Use of Electronic Mail and Internet Guidelines" as of March 26, 2008.

A handwritten signature in blue ink, appearing to read "Kathleen Bellair".

**Chairman
Informatics Policy Committee (IPC)**