

# **Use of Electronic Mail and the Internet**

## **Guidelines for Employees of the Government of the Northwest Territories**

### **Introduction**

The purpose of these Guidelines is to define and explain proper use of the Internet and electronic mail (e-mail) by employees of the GNWT and to provide guidance to employees regarding appropriate use of the government Internet and e-mail systems.

If an employee feels that these Guidelines are too restrictive in any area, and prevents or affects the completion of any task, they should consult with their departmental IT staff. There may be an occasional legitimate need for non-compliance, but not without good reason and departmental support.

In these Guidelines, references to e-mail include: OpenMail (the GNWT corporate e-mail system), Internet e-mail, and any other electronic mail system used by departments, boards or agencies of government for the purpose of conducting government business.

In these Guidelines, "employees" are employees of the GNWT as defined in the *Public Service Act*.

All employees should be aware of these Guidelines and will be provided with a copy. Both new and current employees are required to confirm their understanding of the Guidelines when provided with e-mail and Internet access.

Information about the design and implementation of departmental web sites is the responsibility of the Press Secretary, and is covered in the GNWT Internet Handbook. This includes information on such topics as the Visual Identity Program, HTML specification, page layout, page structure and some technical design considerations.

### **Authority**

The Informatics Policy Committee has issued these Guidelines. The membership of this Committee is made up of the Deputy Ministers of GNWT departments that are major operators and users of information systems. The Secretary to the Financial Management Board chairs the Committee. Comments and questions can be directed to the Manager of Informatics, FMBS.

Departments or agencies may wish to supplement these guidelines to better meet their individual requirements. Such additional requirements shall be at the direction of the appropriate Deputy Minister or Chief Executive.

Individual departments or agencies have the responsibility to ensure their staff conforms to these guidelines. This may require monitoring of e-mail and Internet usage to identify or confirm instances of suspected abuse.

### **Date of Issue**

These Guidelines were issued and take effect March 1, 2000.

### **Principles**

The following principles guide the use of the Internet by employees:

1. Computers, networks, and computing facilities are provided for the performance of assigned duties. The use of this equipment or technology for any other purpose is not appropriate.
2. Employees must comply with these Guidelines, and with any additional standards required by their individual departments.
3. Internet applications that improve the delivery of government programs and services in a cost-effective manner are encouraged.
4. Employees must recognize system and network capacity constraints when using e-mail and Internet services.
5. Provided the above principles are met, it is generally held that information available to the public via the Internet should also be available to government employees.

### **Use of Electronic Mail and the Internet by Staff**

#### **Acceptable Uses**

Access to e-mail and the Internet is provided to employees as tools to increase the overall efficiency and effectiveness of program delivery. E-mail is an effective communication tool which fosters cooperation, teamwork and partnering. The Internet provides access to a wide variety of information, resources and communication tools that can assist employees to perform their jobs.

Employees are encouraged to use both e-mail and the Internet to carry out job responsibilities and to explore new ways providing cost-effective and high quality services to clients.

Job related uses of the Internet include accessing external databases, libraries, newspapers, newsletters, magazines, bulletin boards or encyclopedias to obtain reference information or conduct research; corresponding with colleagues, government clients, and vendors; professional and career development; and provision of information to the public.

Using the Internet for any activities that are not job related (e.g. surfing or browsing for material of personal interest) is not acceptable.

### Information Management

All e-mail and other documents produced on the Internet are considered government records. They are subject to the same information management legislation (*Access to Information Act* and *Protection of Privacy Act*), description and scheduling standards (ARCS/ORCS), and practices to ensure access, integrity, and preservation of public records as other types of government documents. Employees should be particularly aware that this applies to all communications with colleagues, businesses and the general public that are created using government e-mail and Internet services.

### Intellectual Property

The authors of electronic material have copyright and intellectual property rights, unless these rights are explicitly waived. Permission must be obtained from the author before information is used or duplicated. Once permission is obtained, credit must be given to the author.

Employees shall respect intellectual property rights at all times when obtaining information over the Internet.

### Network Etiquette

Employees should observe network etiquette, customs and courtesies, when using e-mail and the Internet.

There are also commonly accepted procedures that should be followed when participating in electronic discussion groups, transferring files from other computers, or sending information to others on the Internet.

IT staff in departments can provide advice or training in network etiquette and related procedures.

### Right of Use

E-mail and the Internet are required by most employees for the performance of their duties. Access, however, is not a right. Both e-mail and Internet access are tools entrusted to the employee. Access to these tools can be revoked at any time for inappropriate conduct. Such conduct may also result in disciplinary action.

### Responsible Use of Electronic Mail and the Internet

The Internet is made up of thousands of interconnected computer networks and systems. Many of these facilities are provided free of charge by governments, universities, public service organizations and companies. As guests on the many networks that compose the Internet, GNWT employees are expected to act responsibly and professionally. This section identifies some of the more common do's and don'ts.

Employees must properly identify themselves when using government e-mail and Internet services. The use of "handles" or other aliases is not permitted in official activities.

Employees must not use an account, signature or signature block other than their own.

Employees should be particularly careful about how they represent themselves when using government e-mail or Internet services. In the conduct of government business, what an employee says or does may be interpreted as GNWT position or policy. The conduct of every employee reflects on the reputation of the government and its staff.

Employees must make appropriate arrangements for their manager or supervisor to access their e-mail accounts during periods (planned or unplanned) when they are absent and unable to respond to messages. It is imperative that normal government operations be maintained.

Inappropriate and prohibited uses of government e-mail and Internet services include:

1. Use of e-mail or the Internet for private business or soliciting money for personal causes.
2. Posting personal web pages.
3. Use of e-mail or the Internet for political lobbying.
4. Use of e-mail or Internet accounts by an individual other than the authorized account owner, and/or use of the account for purposes other than those authorized.
5. Modifying files, data, or passwords belonging to other users, or misrepresenting other users on any network.
6. Use of e-mail or the Internet in such a manner as to disrupt the use of the government's wide area network by others.
7. Use of GNWT computing and communications facilities, including local and wide area networks, to develop or use techniques that harass other users, infiltrate a computer or computing system, intercept private communications, distribute viruses, and/or cause damage to the hardware, software, or data components of a computer system or network.

8. Use of e-mail or the Internet to produce hate mail, harassment, discriminatory remarks, and other antisocial behavior.
9. Use of the Internet to access or download pornographic and/or other offensive material.
10. Use of e-mail or the Internet to send messages that are defamatory or contain abusive or objectionable language.
11. Use of e-mail or the Internet for purposes of misrepresenting oneself or the GNWT.
12. Use of e-mail or the Internet for sending "chain" letters or messages containing large attachments and/or executable files that are not related to GNWT activities or programs.
13. Use of the Internet for accessing on-line games, personal interest chat sites, or streaming videos, or any other activities that could cause congestion and disruption of networks and systems.
14. The use of e-mail or the Internet to conduct any illegal activities.

Internet users can easily download large amounts of information into the GNWT network. This may slow the system's response times for e-mail or file transfers. Any employee considering downloading large files, such as the latest releases of software, should check first with departmental IT staff, to determine the impact on the GNWT network.

Employees must not use new technologies to circumvent any restrictions contained in these Guidelines. In other words, employees must respect the spirit of any restriction put in place. For example, in order to prevent radio or sound clips from tying up network resources and slowing response times, the use of RealAudio in the GNWT network system has been filtered or restricted. While newer releases of Internet browsers make it possible to get around the filtering of RealAudio, it is not appropriate to use them in this manner.

Users must respect all licence agreements when transferring software and information on the Internet, including any agreements that departments have, with the private sector or other government departments, covering the use of software and information. Copyright violation is a serious legal matter. It is everyone's responsibility to comply and ensure that any software that is used within the department is authorized.

### Security and Integrity Issues for Networks and Hosts

Although the GNWT's corporate electronic mail system (OPENMAIL) is secure, e-mail messages sent across the Internet should not be thought of as private communication. Computer hackers are capable of using software called "sniffers" to read, change, and forward e-mail messages and other file transfers. A copy of a word or phrase found in a message or file can be retained before the message or file is forwarded to its destination. For example, any messages containing words or phrases relating to contracts or bids could be intercepted. This information could then be used for fraudulent purposes.

Particular care must be taken when transmitting information that is protected under the Access to Information or Protection of Privacy Act or is otherwise designated as confidential information. Department IT staff can provide advice on encryption techniques.

Employees must use and safeguard passwords. It is recommended that passwords be at least six characters long, random in nature and changed on a regular basis. Do not leave passwords in predictable places, such as desk drawers. Passwords can also be intercepted anywhere in the Internet. Employees should use a different password to sign on to the Internet from that used for signing on remotely to their departmental systems.

There is risk associated with downloading files from the Internet. These files may be infected by a computer virus or contain malicious software code. Documents, data files and executable files are all at risk. Infected files can alter or destroy user or departmental data files, copy password files, or negatively affect GNWT networks.

Employees are responsible for ensuring that any file downloaded from the Internet is free of viruses prior to its use. Each department should have an approved, licensed copy of anti-virus software available for the use of employees. To find out more about the use of anti-virus software, contact your departmental IT staff.

#### Unsolicited Internet E-mail

Employees may occasionally receive unsolicited Internet mail or "electronic junk mail". It is almost impossible to entirely prevent these types of messages from getting delivered to GNWT e-mail users. Employees are advised to ignore and delete unsolicited e-mail. Employees must not take action on their own against unsolicited e-mail. This may result in security risks to the corporate network.

Objectionable or offensive messages should be immediately reported departmental IT staff who can take appropriate action.

Employees must not generate electronic junk mail.

Employees may occasionally receive mis-addressed e-mail. As in the case of non-electronic mail, employees are expected to use discretion and good judgement in handling such messages. The sender should be immediately notified of the error.

#### Using Remote Computers (TELNET)

GNWT users are guests on another institution's machine when using TELNET to access remote computer systems. To ensure that the system works well for all users, GNWT users are asked to observe the following courtesies:

- Log off a remote computer system when finished. Maintaining a connection that is not actively used may prevent others from connecting.
- Read or obtain instructions or documentation files when using a system for the first time (usually labeled README).
- Be aware of time and resource limitations of remote systems. Observe any stated restrictions.

### File Transfer Protocol (FTP)

GNWT users are also guests on other systems when using FTP. To ensure that the system works well for all users, GNWT users are asked to observe the following courtesies:

- Login as "anonymous" and respond to the PASSWORD prompt with your electronic mail address, unless the system specifies otherwise.
- Avoid transferring large files from a remote system during peak business hours whenever possible – when in doubt, consult departmental IT staff.
- Be aware of time and resource limitations of remote systems. Adhere to any stated restrictions.
- Remove files transferred to shared system areas as soon as possible. Copy the files to local disks if needed for future use.
- Check transferred files for viruses. Do not use infected files. Report any instances of infected files to your departmental IT staff.
- Respect copyright and licensing agreements of transferred files.

### **Providing Information and Services using the Internet**

#### Responsibilities

In general, designated department officers and managers have the same responsibility and authority to approve the distribution of information over the Internet as they do for information in hard copy format. Specific authorities may vary from department to department.

Each department is responsible for determining the most appropriate way to distribute information using the Internet. An official spokesperson should be identified for each department and listed for clients seeking further information. Employees should consult their supervisors if they are unclear about these authorities.

#### Partnership Guidelines

The GNWT may participate in projects and programs with external organizations and agencies. When the partnership requires the joint use of the Internet, it is recommended that these Guidelines be discussed with and adopted by the partner organizations.

**ACKNOWLEDGEMENT**

Use of Electronic Mail and the Internet  
Guidelines for Employees of the Government of the Northwest Territories  
(GNWT)

I, \_\_\_\_\_, acknowledge that I have read and understand the provisions of the GNWT policy entitled “Use of Electronic Mail and the Internet – Guidelines for Employees of the Government of the Northwest Territories (GNWT)” and that I did so on \_\_\_\_\_, 20\_\_\_\_. I further acknowledge and understand that if I fail to abide by the terms and conditions of this policy, I may be subject to disciplinary action, up to and including dismissal.

DATED this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_,

\_\_\_\_\_  
Signature of Employee