4.3 Guidelines for the Use of the Internet

Disclaimer

This is an adaptation of a document produced by the Internet Working Group of the federal department of Public Works and Government Services Canada (PWGSC). It is reproduced here, often verbatim, with the permission of Mr. Bruno Kierczak, Departmental Chief Information Officer, PWGSC.

Introduction

The use of the Internet by the government for the delivery of information, programs, and services touches on a wide range of issues. This document provides guidelines for situations and issues that government staff may encounter. If departmental Internet policies differ from these guidelines, then the policy must be followed.

Information about issues that are the responsibility of Communications Nova Scotia such as the Visual Identity Program, HTML specification, page layout, page structure, and some technical design considerations are covered in a separate document.

General Use Principles

Government employees should have access to Internet services based on the following four principles:

- Information available to the public on Internets should also be available to government employees, especially those involved in the delivery of associated services.
- Internet applications that enable service delivery and other business and that are supported by a business case analysis should be fostered.
- Access limitations should be dictated by system and network band width requirements.
- Users should follow security guidelines.

Use of the Internet by Staff

In compliance with these Internet guidelines, employees are encouraged to explore the use of Internets to further the government's mission in a cost-effective manner, to provide service of the highest quality to clients, and to discover new ways to use these resources to enhance service delivery.

ACCEPTABLE USES

Business Uses

Government employees should use the Internet, when appropriate, to accomplish job responsibilities more effectively.

The Internet provides access to a wide variety of information resources that can aid employees in the performance of their jobs. Examples of job-related use of the Internet are accessing external databases and files to obtain reference information or conduct research; corresponding with government's clients; disseminating documents to individuals or groups; and participating in and reading discussion groups on job-related topics.

Professional Development

Employees may use the Internet for professional activities and career development.

The Internet may be used to pursue professional and career development goals. Examples of professional uses include communicating with fellow members of committees in professional organizations; collaborating on scientific studies and articles; connecting to resources that provide information relating to career and education opportunities; and participating in and reading electronic mail discussion groups on professional or future career development topics. Contact and participation in technical, scientific, and policy organization activities stimulate staff interest and hence enhance the government's efficiency.

Use of the Internet for professional activities and career development need not be directly related to one's current position, rather it may relate to the full range of professional, technical, and policy issues of interest to the public service.

If billable Internet services are encountered by employees during professional development activities, employees should check with their supervisor to see if the costs can be covered.

Personal Use

At their supervisor's discretion, employees may use the Internet on personal time at work in accordance with the conditions governing access to their work areas. Personal time includes lunch time and the time before and after work.

Employees who use the Internet on personal time can enhance their knowledge of electronic information resources and sharpen information technology skills. Internet use provides cost-effective self-training opportunities. By encouraging the exploration of the Internet on personal time, the government builds a pool of Internet-literate employees who can guide and encourage others.

For personal use, billable Internet services are the employee's responsibility, and arrangements must be made to reimburse the government.

Training Requirements

Supervisors are encouraged to identify Internet training needs and resources, to support staff attendance at training sessions, and to permit use of official time for maintaining skills.

While there is a cost for permitting employees to attend classes, in the long term such training provides benefits—employees will be better informed about Internet resources and how to use them. Employees should be encouraged to attend an overview course, at the supervisor's discretion, in order that they may develop a better understanding of what the Internet is and how it can be used. When appropriate, supervisors should work with employees to determine the need for attending more comprehensive training courses.

As a follow-up to any Internet training session, employees will need to use the Internet in order to develop and maintain skills learned in the class. Within one week of the training, employees will need at least two hours of official time to practise the techniques learned. Supervisors should schedule this time so that other job tasks will not interfere with this important training reinforcement. Supervisors should allow occasional practice time on a continuing basis.

Orientation/familiarization sessions should be arranged through your departmental Information Technology Corporate Service Unit (IT CSU). This includes instructions on how to use Internet electronic mail, the use of client tools (i.e., browsers, newsreaders, search tools), and techniques for effectively finding information. More specialized training in such areas as Hypertext Markup Language (HTML) document generation, and advanced search techniques should be arranged as demand warrants.

Business Development

At the discretion of their supervisors, employees may use official time to attend meetings and programs related to furthering government objectives using Internets.

Programs and workshops help to increase awareness of the valuable resources available over the Internet. For example, the Internet Focus Group has meetings on a wide range of topics. These meetings would supplement the knowledge that can be gained through formal training courses, serve as an avenue for continuing education, and provide a forum for employees to meet others with similar problems and needs in order to share information and solutions.

EMPLOYEE OBLIGATIONS

Privacy and Security

Employees have an obligation to be aware of computer security and privacy concerns and to guard against computer viruses.

All Internet users should be provided with this document and should be required to acknowledge these guidelines when acquiring Internet access. On a broader scale, these are best practices that apply to use of the network in general and should be part of departmental security precautions. Additional guidance and interpretation may be obtained from IT CSUs. However, in general, the guidelines for use of the government's Internet equipment and services are no different than for the use of the telephone, fax, or copier.

Information Management

Employees must follow accepted information management policies and procedures for Internet documents.

With Nova Scotia Government staff using all forms of Internet services to communicate with colleagues, the public, and businesses around the world, it should be understood that documents produced on Internets, including e-mail, are considered government records. They are subject to the same information management legislation (*Government Records Act* and the *Freedom of Information and Protection of Privacy Act*); description and scheduling standards (*STAR/STOR*); and practices (to ensure access, integrity, and preservation of public records) as internal departmental documents.

Intellectual Property

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

Unless the right is explicitly waived, authors of electronic material have copyright and intellectual property rights. Permission must be acquired before duplicating information. Once the author's permission is obtained to use the property, credits must be included.

Netiquette

Employees must conform to the specific rules of etiquette or established usage policies for each of the available Internet services.

Employees have an obligation to learn about network etiquette (netiquette), customs, and courtesies. Accepted procedures and guidelines should be followed when using electronic mail communications, participating in electronic discussion groups, using remote computer services, transferring files from other computers, or disseminating information to others on the Internet.

Any training program developed by departments for the Internet should include discussion of responsible network use.

Right of Use

Use of the Internet by employees is a privilege, not a right.

Inappropriate conduct or failure to abide by these guidelines could result in loss of Internet access and could result in disciplinary action. Access may be revoked at any time for inappropriate conduct. All employees are responsible for complying with the policies, guidelines, and standards, as set out by the Nova Scotia government.

RESPONSIBLE USE OF THE INTERNET

Use of the Internet encompasses many different interconnected networks and computer systems. Many of these systems are provided free of charge by governments, universities, public service organizations, and commercial companies. Each system has its own rules and limitations, and guests on these systems have an obligation to learn and abide by the rules.

Users must identify themselves properly when using any Internet service: the use of “handles” or other aliases is not permitted in official activities. They must not use an account, signature, or signature block other than their own. Users should also be careful about how they represent themselves, given that what they say or do could be interpreted as Nova Scotia government opinion or policy. Users must be aware that their conduct can reflect on the reputation of the government and its employees.

Examples of inappropriate and prohibited conduct include:

- use of the network for private business or soliciting money for personal causes
- use of the network for political lobbying
- use of a network account by an individual other than the authorized account owner and/or use of the account for purposes other than those authorized
- modifying files, other data or passwords belonging to other users or misrepresenting other users on any network
- use of the network in such manner as to disrupt the use of the network by others; hardware or software shall not be destroyed, modified, or abused in any way
- malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system
- use of the network to produce hate mail, harassment, discriminatory remarks, and other antisocial behaviour
- use of the network to access or process pornographic and/or other offensive material
- use of abusive or objectionable language in either public or private messages.
- misrepresentation of oneself or the department
- sending "chain" letters
- any other activities that could cause congestion and disruption of networks and systems

ELECTRONIC MAIL AND FILE STORAGE AREAS

The content and maintenance of a user's electronic mailbox and shared file storage areas are the user's responsibility.

- Users should check electronic mail at least daily.
- Users should use a signature block at the bottom of electronic mail messages. Signature blocks should be short, preferably not more than six lines, and should include the user's name, electronic mail address, and postal address; a phone number is optional. GroupWise users can use a text editor to create a signature file containing the user's signature block and then include this file at the end of e-mail messages destined for the Internet by use of the GroupWise "File Retrieve" (F11) function.

- Users must add a disclaimer to the signature block when not officially representing the department if the message could be perceived as Nova Scotia government business or as an opinion. An example of a disclaimer is: "The opinions expressed here are my own and do not necessarily represent those of the Nova Scotia government."
- Users must be aware that unless encrypted, electronic mail to the Internet is not private communication, because others may be able to read or access mail. Electronic mail may best be treated as if it is a postcard rather than as a sealed letter.
- Users should delete unwanted messages or files that are not government records immediately, because they take up disk storage space.

Dealing with Unsolicited Mail

Employees receiving unsolicited mail must advise their Information Technology CSU. "Flaming" or similar arbitrary action is prohibited as it could present risks to the corporate network. Similarly, employees should not generate wide distribution electronic mail ("spamming") that could generate negative reaction and impact network performance.

Electronic Discussion Groups

Staff members who participate in electronic discussion groups (ListServs, UseNet newsgroups, etc.) should learn and abide by the rules and etiquette of those groups. Just as different groups of people vary in their expectations, the rules and etiquette may vary among discussion groups. Some general guidelines are:

- Retain initial welcome messages/information files received when first subscribing to a discussion group (for example, instructions on how to unsubscribe).
- Observe the conventions and particular interests of the group prior to becoming an active participant.
- Use signature blocks at the bottom of electronic mail messages.
- When not officially representing the department, add a disclaimer to the signature block.
- Keep messages short and to the point. Generally limit messages to one subject.
- Act in a professional and courteous manner. Avoid gossip and remember that statements about others may find their way back to them. Be patient with new users.

- Be clear and concise. Reread messages before sending them to be sure they will not be misunderstood. Read all messages carefully before responding.
- Be aware of the potential audience in any discussion group and address them accordingly.
- Be careful when using sarcasm and humour. Identify intended humour with standard statements [e.g.,'only joking folks'] or with symbols [e.g., :-) smiley face].
- Cite all quotations, references, and sources.
- Limit line length to fewer than 80 characters because many systems cannot display longer lines.
- Use capitalization sparingly. Capitalizing long portions of a communication is called "shouting" and is considered rude. *Asterisks* or _underscore_characters_ can be used to make a stronger point.
- Use discretion when sending long documents to discussion groups. It is preferable to reference the source of a document and provide instructions on how to obtain a copy.
- Do not forward personal electronic mail messages to discussion groups without the original author's permission.
- Respect copyright and licensing agreements.
- Include only the relevant portions when quoting from a previous message. Clearly identify the quoted portions.
- Learn abbreviation conventions and network jargon. Be aware that these may vary from one discussion group to another. Some common examples include: BTW for "by the way" and IMHO for "in my humble opinion".

Using Remote Computers (TELNET)

When using TELNET to access remote computer systems, users should remember that they are guests on another institution's machine. To help ensure that other Internet users have access to the same information in a timely manner, remote users should observe a few basic courtesies:

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

File Transfer Protocol (FTP)

As with TELNET, users are guests on other systems. To ensure that other Internet users have access to the information, a few basic guidelines should be followed:

- Log in as "anonymous" and respond to the PASSWORD prompt with your electronic mail address, unless the system specifies otherwise.
- Avoid transferring large files during peak business hours from a remote system whenever possible.
- 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.
- Transfer files directly to diskettes rather than to the hard drive if possible. Check transferred files for viruses. Do not use infected files.
- Respect copyright and licensing agreements of transferred files.

Providing Information and Services on Internets

RESPONSIBILITIES

In compliance with these guidelines and within their organizations and program areas, designated authorities have the same responsibility and authority to approve the dissemination of information over Internets as approving the dissemination of information in hard copy format. Each organization/program shall be responsible for devising the most appropriate way to pursue electronic dissemination of information using Internets. Departmental management, based on content, shall designate the appropriate level of authority needed for approvals. An official spokesperson should be identified and listed for clients seeking further information.

PARTNERSHIP GUIDELINES

The government actively participates in projects and programs with external organizations and agencies. It is recommended that these Guidelines for the Use of the Internet in the Nova Scotia Government be adopted by government partners in shared Internet activities.

Nova Scotia Government partners are defined as (a) those Canadian non-profit organizations who are engaged in similar and/or related activities or (b) other government departments and agencies, who deliver programs and services via a delivery agreement with the Nova Scotia government or (c) agents of the province: anyone working on behalf of the province e.g., private companies with active government contracts.

ADDING FILES TO THE NS GOVERNMENT WWW AND FTP SERVERS

The Nova Scotia government provides several WWW and FTP servers, both on the Internet and on the government's network for the purpose of hosting FTP and WWW sites for government departments, agencies, committees, etc.

Both WWW and FTP sites can be public or password protected. A public WWW site serves information to a WWW browser such as Microsoft Internet Explorer, Netscape Navigator, or Mosaic without any request for identification. If required, WWW sites can be set up to request a user ID and password. FTP allows the uploading and downloading of files and documents. A public FTP site is known as an anonymous FTP site. The common username of "anonymous" is used, along with the user's e-mail address as the password.

Space will be provided for the dissemination of information that meets the following guidelines:

- The stored information is sponsored by an organization/program within the Nova Scotia government or by one of the Nova Scotia government's partners. The sponsor confirms that the information meets the criteria below. The sponsor provides operational staff with a contact in the event that a system problem arises or an abuse of the network is detected.
- The sponsor must accept responsibility for resolving claims about copyright or patent infringement and adhere to the policies of the Government of Nova Scotia in this regard.
- Storage space is not unlimited. Some estimate of the size of the community of interest must be provided for large sites.
- The stored information furthers the mission of the Nova Scotia government.
- The stored information conforms to network acceptable use policies of the Nova Scotia government and of any networks of which the Nova Scotia government is a member.

- In situations where the stored information is interfering with normal operation of the computer system or network, operational staff will notify the sponsor (or contact person).
- Documents and files placed on government servers may be of any format, e.g., HTML, graphics, WordPerfect, text, executable. The extension of these files should indicate the type of file and use commonly accepted standards such as .htm, .gif, .jpg, .wpd, .txt, .exe.
- Sites must only contain files that are to be served. Old versions, backups, source documents, templates, etc., must not be loaded onto or left on a site.
- The stored information must be maintained on a timely basis.
- Web sites must conform to any applicable government design, content, and management standards.

Security and Network Integrity Issues for Networks and Hosts

Issues within this area are being addressed through various security initiatives of the Nova Scotia government and on a case-by-case basis dealing with specific needs to deliver services to outside clients. This area represents a new policy frontier, and efforts must be made to develop guidelines in a "proactive" manner to meet the future needs of the Nova Scotia government.

The user should understand that, unless suitably encrypted, Internet e-mail is not a "private communication" and that others are able to read, alter, and forward received e-mail messages. E-mail addresses often have the departmental address attached to them, thus the contents of the message reflect directly on the department. At present, unless a product such as PGP is used, there is no effective way to authenticate the originator of a message or to be assured that an e-mail message was not intercepted and changed.

Communications via e-mail should be informative, polite, and concise, reflecting the same tone and manner used in traditional correspondence.

Users should also be aware that unscrupulous people may run programs on Internet nodes that monitor all traffic going through them, looking for pre-set words or phrases. If a word or phrase is found in a message, then a copy is filed before the message is forwarded to its destination. For instance, any messages containing words or phrases relating to contracts or bids could be intercepted. This information could then be used for fraudulent purposes.

Departmental e-mail practice should be that classified and extremely sensitive designated information are not to be transmitted via Internet e-mail unless encrypted, or protected by other methods approved by the department. E-mail within the internal GroupWise government system is automatically encrypted.

Users accessing remote systems are able to download data and executable files. Such files may have been infected by a computer virus or contain a malicious software code that might destroy user or departmental data files, copy password files, or negatively affect the local area network. Any file downloaded from a Internet, whether a data or an executable file, must be scanned for viruses prior to its use. Even a document file can contain a virus. The department does maintain an approved, licensed copy of an anti-virus software package that is available to all employees. To find out more about its use contact your Information Technology CSU.

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

Passwords used to sign on to various Internet services may be intercepted anywhere along the network. Users should use a different password on the Internet from that used for signing on remotely to their departmental systems. Employees should safeguard passwords and not leave them in predictable places, such as desk drawers. The passwords should be at least six characters, random in nature, and changed on a regular basis.

The Nova Scotia government network is protected against unauthorized access from the Internet by a security host called a "firewall." In general, no access is allowed to the government network from the Internet. Controlled access from the Internet to TELNET, FTP, and certain other services on specific computer systems on the government network can be granted in some circumstances. Contact your Information Technology CSU for information.

Logging of Activities

One of the features the Nova Scotia government firewall provides is logging of Internet activities. Only the firewall administrator has access to these logs. These logs can be viewed in the event of any suspected abuse of privilege or security violation.

It is important from the end user point of view to know that this facility exists, but equally necessary to ensure there are safeguards to protect the user's privacy.

Appendices

Appendix 4-A: Acronyms and Definitions

Appendix 4-B: NS Government Internet: Frequently Asked Questions (FAQs)

Enquiries

Corporate Strategist (Information Management)
Policy and Strategy Division
Office of Economic Development
(902) 424-2915

Approval date: March 1, 2000	*Manual release date: January 9, 2003*
Approved by: Deputy Minister, TSS	*Most recent review: April 18, 1997*

Appendix 4-A

Acronyms and Definitions

BBS: BULLETIN BOARD SYSTEM
A specific mode of electronic access involving dial-up access to a single computer (or computer network) for access to a select and defined information or service set.

EC: ELECTRONIC COMMERCE
Term denoting a range of electronic transfer mechanisms involved in the transfer, request, and authorization of transactional computer network interactions.

EDI: ELECTRONIC DATA INTERCHANGE
Methods for the secure transfer of documents and funds as in electronic commerce.

FIREWALL
Electronic security system deployed between two networks to control access and data flow in both directions.

FTP: FILE TRANSFER PROTOCOL
Protocol established for the electronic transmission of files. Internet world-wide network of computers and computer networks connected to each other using standard communications protocols.

INTRANET
Internal Internet services to support corporate activities within the firewall.

LAN: LOCAL AREA NETWORK
A small computer network connecting and servicing computers in a defined area, usually a single building or group of buildings.

SGML: STANDARD GENERALIZED MARK-UP LANGUAGE
An International Standards Organization (ISO) standard specifying a platform-independent method for storing and printing electronic information.

TELNET
Method for logging on to a remote computer using Internets and/or telephone circuits.

WAN: WIDE AREA NETWORK
An interconnected network that spans a wide area including countries and the globe.

WWW: WORLD-WIDE WEB
A hypertext-based system application for locating and using Internet sources.

Appendix 4-B

NS Government Internet: Frequently Asked Questions (FAQ)

What is the Internet?

The Internet is a system of interconnected networks that spans the world representing 70 countries, 24,000, networks and 2.2 million hosts. Internet growth in the last year has reached 10 per cent per month or a new network every 20 minutes.

Does the Nova Scotia government have Internet access?

Yes, the Nova Scotia government became connected to the Internet by subscribing to iStar, an Ontario-based Internet Service Provider. For the most part, any person connected to the Nova Scotia Government Wide Area Network can be set up to be an Internet user.

What is required to get Internet access?

In general, the user needs to be connected to a LAN, have a properly assigned IP address, and TCP/IP software for the workstation. Consult your LAN administrator or IT CSU staff for information.

What's out there for me?

There is something for everyone on the Internet. But finding it is the challenge for the novice user. To assist, both on-line and text documents will list places to start and focus on using various search tools to allow users to find the information they need.

INTERNET DIRECTORIES AND INDEXES

Internet directories such as Yahoo Canada and indexes such as Altavista are excellent places to start looking.

NEWSGROUPS AND MAIL LISTS

There are newsgroups and mail lists devoted to a multitude of topics, from law to computers to hobbies. Finding those that match your business interest will enable you to keep up to date, to exchange ideas with others, and to benefit from a pool of expertise.

E-MAIL

GroupWise users can use the Internet gateway to exchange e-mail with other Internet users. Use the word "Internet" followed by a colon in the "To:" section of the e-mail address block, i.e., Internet:username@location.

SITE DIRECTORIES

Many sites list their services and programs, their key contact persons, and telephone numbers.

SOFTWARE

Whether from a vendor or a university or government, the Internet provides instant access to software which can be downloaded.

How are others using the Internet?

Getting information in a timely manner is a key to success today. That is the major use for the Internet in the Nova Scotia government. As well, the Nova Scotia government has Internet services whereby information on departments, mandates, services, branches, contact persons, and products will be posted and made available. Thus Internet is a two-way street. Other governments are experiencing the same rapid growth in Internet interest and usage. Some departments are already doing business and providing services on the Internet.

Where can I find training?

Contact your Information Technology CSU. There are also many training resources and self-directed courses available on the Internet itself.

Do I pay usage fees?

Not at this time, you can use the Internet as much as required.

How do I get connected?

Users wishing Internet connectivity should call their Help Desk or contact their Information Technology CSU. Special Internet software must be installed and configured.