1. STATEMENT

Internet access is provided to Government of the Northwest Territories (GNWT) employees as a tool 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 Internet use, explain the impacts that it can have on shared technology resources, and provide clarity on related security 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").

This policy applies to all employees of the GNWT in all Departments, Boards and Agencies, except employees of the NWT Power Corporation.

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 Internet use within their respective departments and ensuring adherence to all related policies and standards.

Employees/Users are responsible for exercising common sense and good judgement when using the Internet so that their actions are not illegal, do not degrade the performance of shared technology resources or compromise their security, or cause incremental expense to the GNWT.

Managers/ Supervisors are responsible for requesting and documenting access to restricted websites on behalf of employees, and initiating action regarding inappropriate Internet use as per the Code of Conduct.

The Department of Public Works and Services (PWS), Technology Service Centre (TSC) is responsible for providing Internet access and for monitoring and reporting on Internet 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 - Internet access is provided as a tool for work-related activities such as conducting research, keeping up to date on current developments and best practices related to assigned work, participating in work-related professional development activities, communicating and sharing information with colleagues, and providing government services to the public.

2. Privacy – Network use, including use of the Internet, is monitored and regularly reported to Deputy Heads. Users should have no expectation of privacy when using the Internet. Information created using government computers, facilities, networks or resources (including Internet access) is considered a government record and can be accessed by the public under the Access to Information and Protection of Privacy Act (ATIPP). This may include, for example, information from the Internet or records of Internet access by a user.

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

   (Reference: Electronic Information Security Policy #6003.00.26)

4. Personal Use – Limited and occasional personal Internet use is permitted under the Code of Conduct provided it does not negatively impact the performance of work responsibilities. Employees are expected to use common sense and good judgement when using the Internet so that their use does not negatively impact shared government resources or create incremental expense to the GNWT and to seek further guidance from their Supervisor if they are uncertain about appropriate use.

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

a) Conducting illegal activities. This includes copying and sending confidential or proprietary information or software that is protected by copyright and other laws protecting intellectual property, and maliciously or knowingly spreading viruses. Illegal activities will be promptly reported to the RCMP for investigation.

b) Accessing websites supporting hate, pornography, gambling, shopping or auctions, investments or stock trading, gaming, espionage and terrorism, theft, or drugs, unless accessing such sites is a requirement of your job responsibilities and access is authorized.

c) Transmitting or downloading material that is discriminatory, defamatory, harassing, insulting, offensive, pornographic or obscene.

d) Participating in activities, including the preparation or distribution of content that could damage the government's image or reputation.

5. PROCEDURES

1. Employees requiring access to restricted web sites (as per the Code of Conduct) as part of their job responsibilities must have their manager or supervisor request access from the TSC. The TSC may arrange temporary access to a government computer that is not on the GNWT network as current filtering methods do not allow for individual computers to be unblocked – if a site is unblocked for one person, it is unblocked for all.

2. Employees should stop using the Internet for any personal usage and reduce business usage (as operational situations allow) when they receive advisories from the TSC that network performance is degrading. The TSC may limit access to some shared resources in order to ensure continued operation of critical GNWT applications.

3. The following activities are not allowed (exceptions noted) because they present either a security risk, can negatively impact network performance for all users, or have the potential to cause additional expense to the GNWT:

   a) Non work-related streaming audio or video.

   Exceptions:

   - Work-related access to streaming audio and video is permitted. Employees are reminded that streaming audio or video files use significant bandwidth with each connection and can degrade network performance. Where feasible, employees are encouraged to initiate such downloads at the end of the day or at noon when the network is usually less busy.

- Departments that wish to incorporate streaming audio or video technologies for work purposes are encouraged to consult with the TSC in order to select the most appropriate methods to minimize network and other resource impacts.

b) Non work-related use of peer-to-peer voice over IP (VOIP) or desktop-based videoconferencing services over the Internet.

Exceptions:

- Departments that wish to use VOIP or desktop-based videoconferencing for work purposes are encouraged to consult with the TSC in order to select the most appropriate technologies to minimize network and other resource impacts.

c) Non work-related use of a government computer as a file server for sharing files.

d) Downloading attachments from personal Webmail (e-mail) accounts to government computers – this activity presents a limited security risk by introducing viruses into the network environment. (Note: GNWT desktop computers are protected with anti-virus capabilities and updated regularly, but risk occurs when security measures are circumvented or compromised e.g. users disabling desktop level protection or when anti-virus protection is not up-to-date on laptops that are only used occasionally.

e) Attempting to disable, defeat, or circumvent any government security facility such as the firewalls, proxies, Internet address screening programs and other security systems that have been installed to assure the safety and security of the network.

4. Employees who violate this policy may be subject to disciplinary action up to and including dismissal.

6. SUPPORTING DOCUMENTATION

Document References

Document Title	*Reference*
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.
Electronic Information Security Policy	IPC Policy #6003.00.26
Electronic Information Security - Standards of Best Practice for Information Security Management	IPC Policy #6003.00.27 • Information Processing: IP 2.3 - Workstation Configuration (pg. 65) • Information Processing: IP 4.8 - Access Logging (pg. 82) • Security Management: SM 5.1- Malicious Code (pg. 22)

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.

Kathleen McClain

Chairman
Informatics Policy Committee (IPC)