Government of Yukon
Guidelines for Using YESNet and YNet Computers

1. Introduction

Computers and electronic networks are important government assets used to improve the delivery of services to the public. Government of Yukon provides access to these computer resources so that employees and other people authorized to use these resources can:

- conduct the business of government through efficient internal/external communications with other individuals, organizations and the public;
- conduct research, gather and share information relevant to their duties; and
- take up opportunities to improve technical skills and acquire knowledge.

Most people will use these assets in a responsible manner. As with any innovative tool, however, there is the possibility that it can also be used in a manner for which it was not intended. People who are authorized to use these resources must not hinder the productivity or job performance of employees, damage the ethical and professional behaviour of the public service, impair the security and integrity of the government's information holdings and network resources or jeopardize the legal position of the government.

2. Purpose

These guidelines:

- describe the key principles for the appropriate use of computers and electronic networks;
- define the roles and responsibilities of users, their supervisors, and other key stakeholders; and
- provide examples of acceptable and unacceptable use.

3. Scope and application

These guidelines do not cover every acceptable and unacceptable scenario. They draw on common sense and basic public service principles for authorized users and supervisors to determine appropriate computer use activities in the work place.

These guidelines apply to all departments, as defined in Policy 1.1 of the General Administration Manual (GAM) including employees, confidential exclusions, contractors, appointees, trainees and other personnel using government computers and electronic networks during normal working hours and all other times.

These guidelines apply to all authorized users who access computer resources and services from government computers, including Yukon Public School computers and servers. They also cover authorized users while they are using their own equipment (including home computers), or equipment belonging to a third party, to access the government network for work purposes.

The nature of some specific government job functions may require accessing information that would not conform to the guidelines (e.g. health care, criminal investigations, law enforcement) and are therefore exempt.

Separate guidelines are in place for the e-mail distribution of Global Notes.

4. Principles of use for computers and electronic networks

These principles will help authorized users determine what is appropriate use of computer resources. Appendix 1 lists examples, but the underlying premise is that any activity must be able to survive public scrutiny through the taxpayers' eyes without bringing the public service or the government into disrepute.

See Appendix 1 for details on these principles.

Principle 1:
Users have a responsibility to protect IT investments
and government information.
Authorized users will not compromise the security, confidentiality and performance of the government's telecommunications and network infrastructure and information.

Principle 2:
Users are accountable to the public.
Authorized users must not use computer resources to conduct activities that will bring the public service into disrepute or be detrimental to its ethics, professionalism, integrity, standards of etiquette or productivity.

Principle 3:
Users are committed to upholding all legal and policy obligations.
Authorized users are obligated to ensure that the use of computer resources does not violate the Criminal Code of Canada, other federal laws or regulations, Yukon laws including the Yukon Human Rights Act or Yukon government policies and guidelines.

Principle 4:
Users may occasionally use government computers and electronic networks for acceptable personal or educational activities.
In this electronic and information age, some incidental and occasional personal use of computer resources is permitted if the use is reasonable in duration, does not result in increased costs and is consistent with these principles and these guidelines.
Personal or educational use of government computers, e-mail and internet services must not negatively affect the professional image of the public service, detract from the work duties and productivity of employees, or be used for private business operations or personal financial gain.

5. Privacy of information

The Government of Yukon owns information and records stored or transmitted on its equipment and information systems. Authorized users need to be aware that they do not have a right of privacy in their use of electronic networks and corporate computers.

Authorized personnel will investigate and monitor an individual's activities only if it is suspected that one or more of the four principles are not being followed.

Activities using computers and electronic networks that would contravene the *Access to Information and Protection of Privacy Act* are not permitted.

Any disclosure of information collected or accessed through either general or specific monitoring will be in accordance with the requirements of the *Access to Information and Protection of Privacy Act*. Some job functions in specific program areas such as health, justice and education must protect the client relationship. Privacy and confidentiality in these situations will not be compromised.

6. Roles and responsibilities

Authorized users

Authorized users are responsible for:

- reading and understanding these and other guidelines or corporate policies for the use of computer resources and conforming to them;
- reading, signing and agreeing to the terms of the YNet Account Application form;
- reading and agreeing to the terms of the YESNet Guidelines for Computer Use
- ensuring their use of computers and electronic networks is consistent with activities identified in all Government of Yukon policies and other guidelines [e.g. Oath of Office, General Administration Manual (GAM) – *Conflict of Interest Policy* (Policy 3.39), *Workplace Harassment Policy* (Policy 3.47), *Speaking in Public and Writing for Publication Policy* (Policy 1.4)]*;*
- taking reasonable security measures to protect the use of their passwords for accessing computer accounts and systems;
- ensuring that sensitive, confidential or personal information residing on PCs, laptops and servers is secure and safeguarded at all times;
- taking precautions to avoid transferring computer viruses onto the network;
- respecting intellectual property rights at all times when using computer resources;
- advising their supervisor or Highways and Public Works (HPW), Information and Communications Technology (ICT) staff of any

circumstances, incidents or events which may impact the availability or performance of the electronic network; and

- when in doubt, asking their supervisor or department human resource unit to clarify whether a contemplated use of the computers and electronic network is unlawful or unacceptable within these guidelines.

Supervisors

The role of the user's supervisor is to:

- determine who within their department requires access to computers and electronic networks, have approved users read and sign the YNet *Account Application Form,* and then authorize this form with their signature as the user's supervisor;
- ensure that all authorized users have read and are continually aware of these guidelines and conform to appropriate computer use through the Global Notes on YESNet's First Class Communications System;
- clarify any questions whether or not a specific activity on a government computer or network would be an offence against a law, a contravention of any policy or these guidelines;
- formally advise ITSS of requests for YNet or TAL for YESNet account modifications or to permanently revoke or temporally suspend a user's access to electronic networks, systems and services upon termination or for investigative or disciplinary purposes;
- manage employees' activities and determine what constitutes a reasonable amount of time spent by staff using computer resources for government business and personal use; and
- investigate or cause to be investigated suspected security breaches, inappropriate or illegal use of the government's computer resources and advise ICT, or in the case of Public Schools Branch, their Director of Learning, of any suspected activities by authorized users.

Information and Communications Technology (ICT), Department of Highways and Public Works

ICT and ITSS, as the central agencies for implementing and managing corporate electronic networks and services, including security, is responsible for:

- ensuring that the most recent release of its corporate anti-virus software products are available;
- managing electronic network user accounts, including identification, authentication and authorization access for YNet or YESNet users;
- monitoring the performance and capacity of electronic networks and systems;
- analyzing network statistics, detecting operational problems in the electronic networks and taking steps to identify the source of the problem which, if authorized by the user's

supervisor, could involve monitoring and analyzing an individual's use of computer resources; and

- advising department officials and the appropriate authorities of suspected unacceptable or illegal activities on a government computer or electronic network.

Public Service Commission (PSC) and department human resource management

Department human resource management and the PSC, as the central agency for human resource management activities, are responsible for:

- ensuring that orientation materials for new employees include a copy of these guidelines;
- distributing any updates to these guidelines or other related materials to department supervisors;
- addressing any questions raised by employees or supervisors if a contemplated activity on a government computer or network would be an offence against any law, a contravention of these guidelines or any internal government policy;
- making endorsed training on the use of computers and electronic networks available to authorized users; and
- issuing periodic department e-mails, Global Notes, or hard copy memos reminding authorized users and supervisors of these guidelines and of their responsibilities when they use government computer resources.

7. Consequences of not adhering to the guidelines

Not complying with these guidelines may result in disciplinary action including oral or written reprimand, limitation or withdrawal of access to computer and network services, suspension or termination of employment. The nature of the disciplinary action will depend on the circumstances and seriousness of the breach of compliance.

Suspected illegal use of a computer or electronic network may be reported to the law enforcement authorities. In such cases the Government of Yukon may take disciplinary measures even where a formal criminal charge or civil lawsuit is not pursued.

Appendix 1

Principle 1:
Users have a responsibility to protect IT investments and government information.

Authorized users will not compromise the security, confidentiality and performance of the government's telecommunications and network infrastructure and information.

Authorized users accessing computers and electronic networks must take reasonable precautions to safeguard government networks, systems, and data. They must also ensure that their activities will not degrade the performance of the electronic network or result in additional or incremental operating costs to the government by:

- downloading unauthorized (not corporately or departmentally endorsed) software, including untested software updates, shareware or freeware, to a computer or network server;
- downloading and/or circulating files on a computer or server without scanning for viruses (incoming e-mails with attachments are automatically scanned);
- opening attachments in personal web-based e-mail (e.g. e-mail accounts from Hot Mail, Yahoo, MSN or any other Internet Service Provider such as YKNet or WHTV) because of associated security risks to the government network;
- compromising sensitive, confidential or personal information residing on PCs, laptops, servers, or printers;
- disclosing sensitive, confidential, business trade secrets, or personal information without authorization in e-mail correspondence;
- disclosing files or data that contain personal, classified or any confidential information in e-mail correspondence to unauthorized recipients;
- attempting to obscure the origin of any message or downloading material under an assumed Internet address;
- improperly using large distribution lists;
- accessing another individual's account without proper authorization;
- divulging, sharing, or compromising Government of Yukon account identifications, passwords, dial-in numbers or other security mechanisms and programs;
- accessing on-line games and personal interest chat sites;
- listening to online radio stations when other options are available (because it consumes significant bandwidth which is an increasing cost for government), downloading music or video files, utilizing unauthorized peer-to peer communications software (e.g. Kazaa) or other activities not associated with an employee's job function that could cause congestion and disruption of the government networks; and
- sending chain letters, greeting cards or other messages containing large attachments or executable files that are not related to the government programs and utilize excessive electronic storage resources.

Principle 2:
Users are accountable to the public.

Authorized users must not conduct activities using computer resources that will bring the public service into disrepute or be detrimental to its ethics, professionalism, integrity, standards of etiquette, or productivity.

Examples of inappropriate activities that would result in negative internal and public feedback include:

- viewing, downloading, or sending inappropriate, offensive, obscene, racist, sexist or sexual content ranging from vulgar to graphic and explicit subject matter in a textual or graphical format, including jokes, cartoons, audio or video clips;
- using government computers or electronic network for furthering outside business interests, personal gain, or profit;
- using government computing resources to engage in political activities, including lobbying on behalf of an interest group;
- using the government's computing resources to engage in on-line gambling;
- accessing on-line games, chat sites, streaming videos, sending chain letters or using inappropriate distribution lists; and
- unreasonable or excessive use of the Intranet or of e-mail for non-business purposes.

Principle 3:
Users are committed to upholding all legal and policy obligations.

Authorized users are obligated to ensure that the use of computer resources does not violate the Criminal Code of Canada, other federal laws or regulations, Yukon laws including the Yukon Human Rights Act or Yukon government policies and guidelines.

The legal position and liability of the government must not be compromised by practices such as:

- making slanderous, offensive, derogatory, or inflammatory remarks that could injure the reputation of any person or group;
- disseminating information or electronic messages that harass, discriminate, abuse, promote hatred or incite violence or cause identifiable groups or individuals to fear for their safety;
- using computers and electronic networks to acquire, store, or distribute pornography;
- criminal offences involving fraud, extortion, blackmail, bribery, illegal gambling, illegal drug dealing, or possession or distribution of explicit sex materials that could lead others to engage in anti-social acts;
- violating copyright, trade marks, patents, and other intellectual property laws;
- downloading and installing unregistered or unlicensed software onto government computers, servers or other equipment;
- developing or using techniques for unauthorized access that attempt to infiltrate a computer system or network, intercept private communications, distribute viruses, or cause damage to hardware, software, or data components of the government's network (e.g. hacking);
- unauthorized destruction, altering or falsifying of electronic public records of the Government of Yukon;
- disclosing without authorization, information that is a mandatory exemption under the *Access to Information and Protection of Privacy Act;*
- representing personal opinions as those of the Government of Yukon or otherwise failing to comply with institutional policies and procedures concerning public statements about the government's position; and
- engaging in any activity that is contrary to any Government of Yukon policy or guideline, including but not limited to the *Oath of Office*, General Administration Manual (GAM) Conflict of Interest Policy (Policy 3.39), Workplace Harassment Policy (Policy 3.47), Speaking in Public and Writing for Publication Policy (Policy 1.4) etc.

Principle 4:
Users may occasionally use government computers and electronic networks for acceptable personal or educational activities.

In this electronic and information age, some incidental and occasional personal use of computer resources is permitted if the use is reasonable in duration, does not result in increased costs and is consistent with these principles and these guidelines.
Personal or educational use of government computers, e-mail and internet services must not negatively affect the professional image of the public service, detract from the work duties and productivity of employees, or be used for private business operations or personal financial gain.

Examples of acceptable computing personal use during an employee's break or outside normal working hours may include:

- studies for personal development from an accredited learning or education institution;
- personal banking or bill payments by using online financial services;
- placing online orders for uncontroversial merchandise from web sites that would not be considered inappropriate, offensive, obscene, racist, sexist, or containing sexual content;
- occasional e-mail correspondence that is not related to government business; or
- occasionally accessing websites for news, weather, or personal interest sites such as CNN, MSN, CBC, etc that would not be considered inappropriate, offensive, racist, sexist, or containing sexual content.