Section: PS 1103

Information Technology Acceptable Usage Policy

Date issued: 1999 06 28

Revision date: 2002 12 11

Purpose

This policy guides users of the Government of Saskatchewan's Information Technology (IT) infrastructure. It balances the employee's ability to benefit fully from information technology with the Government's need for secure and effectively allocated IT resources.

Background

The increasing use of information technology has fundamentally changed the workplace. The Internet, intranets, cellular telephones, fax machines and e-mail have transformed data management and communication and employees utilize this valuable resource in many innovative ways.

The networked office has also created the opportunity to access material and use resources in ways that may not be acceptable. Inappropriate use of information technology could expose the Government to potential embarrassment and possible litigation. The Government is committed to ensuring that this valuable resource is not brought into disrepute in the workplace through inappropriate use. Employees are to follow this policy to ensure that their own use of the Government's information technology resources is appropriate.

Policy

Employees of the Government of Saskatchewan will follow guidelines and policies to enable reasonable and appropriate usage of information systems, and to perform their jobs in accordance with all applicable laws, regulations and policies. The Government of Saskatchewan will periodically redefine and enhance these guidelines and policies.

Government of Saskatchewan policies which apply to:

- freedom of information and protection of privacy;
- harassment;
- performance improvement;
- conflict of interest; and
- corrective discipline.

also apply when employees use the Government's IT infrastructure.

This policy addresses circumstances which are new and evolving, or at least unfamiliar. It augments, rather than replaces, existing Government of Saskatchewan policies.

Employees who violate this policy will be subject to a full range of disciplinary actions.

There are three usage types for the Government of Saskatchewan's IT infrastructure:

- Core;
- Incidental; and
- Unacceptable.

The chart on the last page of this policy provides examples of these three usage types and may be used as a guideline when assessing use of information technology.

The appendices discuss specific applications such as the Internet and e-mail in more detail.

- Appendix 'A' - Internet Use
- Appendix 'B' - E-mail
- Appendix 'C' - On-line discussion groups, Games, Mobile Computing Devices, Data Storage, Voice-Mail, Cellular Phones & Photocopiers

Core

Core uses are activities required to conduct the business of government. They help fulfill the department's mandate. The Government of Saskatchewan's IT infrastructure primarily exists to facilitate Core Government purposes.

Incidental

Incidental uses are those which are neither explicitly permitted nor explicitly denied. Incidental applications never require any action or intervention by anyone at the workplace other than their user. Employees are to cover costs incurred in personal incidental use such as long distance calls or photocopying. Incidental usage that becomes an imposition on others or burdens systems is no longer incidental, but unacceptable, and is not permitted.

Unacceptable

Unacceptable use impedes the work of others or needlessly squanders IT resources. It may unintentionally damage the IT infrastructure, and affect the department's ability to carry out its work. Unacceptable use may generate extra costs. The definition of unacceptable use will vary between departments. However in all cases it is related to the department's mission, vision and values and information needed to perform the work of the organization. For example, access to objectionable Internet sites may be appropriate to specific investigations in one department, but may be unacceptable and not permitted for general use in that department or at any time in another department.

It is unacceptable to:

- Use, copy, or otherwise access anyone else's files without permission.
- Use the Government's information technology infrastructure for activities that contravene the law, existing policies or regulations.
- Use the Government's information technology infrastructure for any activities that are offensive or perceived to be offensive.
- Download data or introduce data from an external source such as a diskette without ensuring that it is virus-checked.
- Use any part of the Government's information technology infrastructure for personal financial gain.
- Infringe copyright or proprietary rights.
- Permit unauthorized access.
- Create or knowingly propagate computer viruses.
- Damage files, equipment, software, or data belonging to others.
- Use or attempt to use unauthorized access methods or abilities.

The above list is not exhaustive.

While the Government of Saskatchewan does not prohibit limited incidental use of information technology for personal reasons, users should recognize that the primary intention of providing this resource is to support the core work of the Government.

It is the policy of the Government of Saskatchewan to ensure that people with hearing, visual and other disabilities have equal access to public information that is available on the Internet and the World Wide Web. It is the direct responsibility of the department and its web page developers to become familiar with the guidelines for achieving universal accessibility and to apply these principles in designing and creating any official Government of Saskatchewan Website. The Government's use of information technology should not create new barriers for people with disabilities. It should be used to reduce barriers and enhance accessibility.

The Government of Saskatchewan's IT infrastructure provides access to outside networks. Employees may encounter offensive or objectionable material. The Government of Saskatchewan does not assume responsibility for the content of any of these outside networks.

Without specific authorization, employees must not cause, permit, or attempt any installation of hardware or software, destruction or modification of data or equipment.

Monitoring

Employees should be aware that computer usage can be traced by site logs and other tracked information. The Government reserves the right to access the contents of all files stored on its systems and all messages transmitted through its information technology infrastructure.

Section: PS 1103

Application

This policy applies to employees appointed under The Public Service Act, 1998 who use any information technology resources which: Are owned by the Government of Saskatchewan or

- Are licensed or leased by the Government of Saskatchewan,
- Connect directly to Government data or telephone networks,
- Connect directly to a computer or other device owned or operated by the Government, and/or
- Otherwise use or affect the Government of Saskatchewan's information technology infrastructure.

This policy also applies to those working under contract to the government who use the Government's information technology resources.

Many departments have their own acceptable usage policies (or some variation thereof). If there appears to be a conflict between the departmental policy and this policy, interpretation should be sought.

Authority

The Public Service Act, 1998

Inquiries

- Departmental Human Resources
- Departmental Communications Branches
- Department Information Technology
- Information Technology Office
- Public Service Commission

Appendices

Technology changes rapidly and its use varies widely between departments. For example, a few years ago personal digital assistants (PDAs), networked photocopiers and workstations with worldwide Internet access were unheard of. Now, they are becoming commonplace in many offices. The list of applications and devices in these appendices is therefore illustrative, not exhaustive. It represents a baseline for acceptable employee usage and may be used as a template for department-specific policies.

Section: PS 1103-A

Information Technology
Acceptable Usage Policy
Internet Use
Appendix A

Date issued: **1999 06 28**

Revision date: **2002 12 11**

If employees have access to the Internet through work, they must not intentionally access sites or engage in practices on the Internet that have the potential to bring the public service into disrepute. Employee access to the Internet is a privilege, not a right. Access entails personal responsibility and employees are responsible for any activity carried out under their account.

Employees who use the Internet should be familiar with:

- Copyright laws as they apply to software and electronic forms of information,
- Applicable libel and slander laws,
- This policy, and
- Their department's policy on Internet use.

The 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. As long as an activity is related to and necessary for the completion of an employee's work, then that activity is generally considered to be an acceptable use of the Internet and is allowed. Individual departmental Internet policies provide further guidance.

The use of the Internet is unacceptable when that use:

- Compromises the privacy of users and their personal data.
- Damages the integrity of a computer system, or the data or programs stored on a computer system.
- Is offensive, or perceived to be offensive.
- Results in personal financial gain for the user.
- Brings the Government of Saskatchewan into disrepute.
- Disrupts the intended use of system or network resources.
- Facilitates unauthorized access attempts on other computer systems.
- Results in the uploading, downloading, modification, or removal of files on the network for which such action is not authorized.

Employees who access the Internet through Community Net have their on-line experience enhanced by site-blocking. Site blocking prevents access to websites in pre-selected categories. When people attempt to visit these sites, a warning screen appears. The software used for site blocking by the Government of Saskatchewan is based on pass-through filtering technology, a very accurate, reliable and scalable method of Internet filtering. The software filters Internet content by working in conjunction with an expanding master database of more than 2.6 million sites organized into more than 75 categories. Blocked categories for Government of Saskatchewan users currently include (but are not limited to):

- Pornography/Adult Content;
- Gambling;
- Racism; and
- Sites that offer web anonymising (proxy avoidance) capabilities.

If an employee attempts to access a website within one of the blocked categories, the request is blocked. Instead of the requested website, a warning screen is displayed on the employee's computer and the incident is logged. These logs are available to the departments' HR Directors.

Information Technology
Acceptable Usage Policy
E-mail
Appendix B

Date issued: **1999 06 28**

Revision date: **2002 12 11**

E-mail that is of a personal or transitory nature need not be archived. However, e-mail that is an official record of government is to be retained. Remember that e-mail is accessible under the terms of The Freedom of Information and Protection of Privacy Act.

Departments should ensure that their e-mail retention policies follow The Archives Act as it refers to official government records.

E-mail is an official record if:

- It was created or received as part of the normal business practices of the department and it relates to the department's mandate,

- It documents, interprets or otherwise supports departmental policy, decisions, transactions and events or it contains informational value of significance to the department.

Employees must not attempt to read another person's e-mail unless otherwise authorized. The e-mail system is the property of the Saskatchewan Government. Employees should have no reasonable expectation of privacy in e-mail transmitted, received and stored on and/or through the government's system. An e-mail is the property of the Government of Saskatchewan and is not a private employee communication (whether created or received).

It is unacceptable to send large files such as singing Christmas cards or animated Valentine's greetings as attachments to e-mail - such attachments can seriously affect the performance of a department's network. Remember that e-mail is the leading source of computer viruses; be especially suspicious of attachments. Unencrypted e-mail is not secure. Employees have a responsibility to put only non-sensitive information in an e-mail. The recipient is responsible for handling the message with respect and securing the sender's permission before forwarding it.

Employees must have their supervisors' permission before using the Government's information technology resources for large scale distribution of e-mail. The e-mail's subject line should always be filled out. Employees are encouraged to create separate signature files for personal and official e-mail that is sent from government accounts. The text of the official signature file must list job title, department and telephone or fax number. Personal signature file text must contain a disclaimer indicating that the e-mail does not represent the views of the Government of Saskatchewan. Signature file size should be kept to a minimum.

Section: PS 1103-B

Many employees access personal or work e-mail through web-based accounts hosted on sites such as HotMail or Netscape. Currently, this incidental use of the Government's information technology infrastructure is permitted. However, web-based e-mail must be used cautiously.

If irresponsible use of web-based e-mail damages departmental computers and networks, permission to access web-based e-mail from work may have to be reviewed.

Employees who access web-based e-mail with Government of Saskatchewan computers, Mobile Computing Devices (ie. Personal Digital Assistants (PDA's)), cell phones and networks are to follow the guidelines below.

- Web-based e-mail account names MUST be different from department network account names.
- Web-based e-mail account passwords MUST not be the same as department passwords.
- Passwords MUST not be words found in the dictionary.
- Passwords MUST contain alpha and numeric characters and be at least 8 characters long.
- Browsers should be configured to prompt the user before external code is run.
- To avoid the inconvenience of logging in and out of web-based e-mail, some websites will ask if you wish to store your password in a browser cache or cookie. DON'T DO THIS. If you do, anyone who has access to your computer can access your account.
- DON'T configure web-based e-mail to automatically forward to work e-mail accounts (or vice versa).
- DON'T forward restricted or confidential work e-mail to your web-based e-mail account.
- Most Web-based e-mail does not include encryption. Therefore, business information, information of a confidential or sensitive nature, such as credit card numbers, passwords and other personal information, should not be sent.
- NEVER open suspicious or unexpected e-mail attachments. They may contain a script or executable program that can delete local files, send files/documents or passwords to another host and severely damage the network.
- DON'T send large attachments.
- Always scan attachments with up-to-date virus software prior to opening.

Information Technology Acceptable Usage Policy
OnLine discussion Groups, Games, Voice-Mail, Mobile Computing Devices (ie. PDA's), Data Storage, Cellular Phones & Photocopiers
Appendix C

Section: PS 1103-C

Date issued: 1999 06 28

Revision date: 2002 12 11

On-Line Discussion Groups

One of the benefits of the Internet is the ability to engage in public discussion groups. When joining in public discussion employees must identify whether they are participating as an individual or a representative of their department. In most cases participation is only appropriate as an individual. Whenever an employee engages in a public discussion through a government account or is identified as being from the government, the government is reflected in what is written. Even though their messages may contain a disclaimer, such messages should conform to the standards of accuracy, courtesy and propriety.

Games

Games are a common feature of stand-alone computers and computers connected through a local area network, an intranet or the Internet. Many office computers come equipped with a few games, solitaire is especially popular. Using Government IT infrastructure to play games during working hours is an unacceptable use of a valuable resource and is not permitted. As well, employees who waste valuable storage space and damage departmental networks by playing multi media games are also using IT resources in an unacceptable manner.

Employees who spend a few minutes playing solitaire over the lunch hour? This is an incidental use but employees are expected to use their common sense and good judgement. As always, "personal use on personal time" is a good rule to follow.

Voice-Mail

Use of voice mail is limited to employees. Employees should ensure their recorded voice mail messages are appropriate, informative and timely. If callers reach your voice mail, at a minimum, they must be able to;

- Speak directly with another employee, or
- Leave a message.

Many departments have their own internal standards that cover areas such as telephone use and client service.

Employees are responsible for the security of their account and their password. They should change their password regularly and take precautions to prevent unauthorized access to their mailbox. Voice mail systems are provided to facilitate the department's core work. Incidental use of voice mail by employees is allowable but should not interfere with, or conflict with, business use. Employees should exercise good judgment regarding the reasonableness of personal use. Employees must not attempt to access others' voice-mail boxes unless specifically authorized.

Section: PS 1103-C

Mobile Computing Devices

Mobile computing devices are all portable computing devices, including but not limited to notebook computers, smart phones, and hand held computing devices (such as Palm Pilot, personal digital assistants, also known as PDA's).

Staff authorized to use a mobile computing device to carryout government business are responsible for protecting the confidentiality, integrity, and availability of government information and information systems. This responsibility includes the device itself, information and information systems resident on the device and information systems that can be accessed from the device.

Staff should ensure that the mobile computing device is protected from theft or removal at all times that the device is not in their immediate possession.

Staff are required to use the security procedures provided with the mobile device to prevent unauthorized access to the device.

Data Storage

Staff should store all government materials, such as data, documents, e-mail messages, spreadsheets, databases, programs, etc. that were received, created or edited on office computers in the course of carrying out government business, on network storage devices (commonly referred to as "the network"). The use of network storage devices will provide for recovery of such materials in the case of loss. Staff are strongly encouraged not to store copies of such materials on office computer hard drives, floppy disks, CD's or other local or removable media unless necessary. Storing materials on such devices exposes government information and information systems to disclosure or unrecoverable loss.

Cellular Phones

Cellular phones are part of the Government's information technology infrastructure:

Telephones and services should only be used to conduct government business.

Agreements should be established to address the use of employee-owned cellular telephones for Government business.

Cellular transmissions are not secure and employees should use discretion in relaying confidential information.

This policy also applies when employees use cellular telephones for e-mail and Internet access.

Section: PS 1103-C

Photocopiers

Photocopiers are part of the Government's information technology infrastructure. An annual licensing agreement exists between the Government of Saskatchewan and the Canadian Copyright Licensing Agency (http://cancopy.com). This agreement permits employees to legally photocopy copyright-protected works in accordance with the federal Copyright Act. Specific questions about the agreement should be directed to departmental administration branches or the Communication Coordination Unit at Executive Council.

Section: PS 1103-sample

Information Technology Acceptable Usage Policy

Date issued: 1999 06 28

Revision date: 2002 12 11

Samples of **Core, Incidental** and **Unacceptable** usage of Government of Saskatchewan Information Technology Infrastructure.

Technology	Core	Core/ Incidental	Incidental	Incidental/ Unacceptable	Unacceptable	Against Existing Policy	Illegal
Phone	Answering an inquiry from a member of the public.		Making a brief personal call.	You make many personal calls & your work calls are answered by busy co-workers	Accessing 1-900 lines on government phones.	Using the office phone during office hours to buy and sell stocks.	Recording phone conversation without permission.
Photocopier	Making copies of a branch meeting agenda.		Making a photo copy of your resume.	Making a photo copy of your neighbour's resume	Extensive personal photo copying that ties up the machine during office hours.	Photo copying brochures that describe a product you sell at the summer fair.	Photocopying and distributing a copywritten article without authorization.
Fax Machine	Sending a revised copy of an office renovation drawing to a contractor.	Using the fax to make personal travel plans that tie in with a work-related conference	Using the fax to confirm the itinerary for your personal travel plans.	Faxing the results of the office hockey pool to the rest of the department.	Faxing out copies of your resume during working hours, tying up the fax & backing up departmental faxes.	Faxing copies of an offensive joke to co-workers in other departmen t	Faxing confidential information to a customer who pays you for it.
Networked Computer	Sending an e-mail to all the members of the department OH&S Committee with minutes of the last meeting.		E-mails to co-workers with birthday wishes, holiday greetings. Playing solitaire while on break.	Sending department-wide e-mails with puppies 4 sale type messages.	Distributing chain-e-mails with large executable file attachments that waste limited network resources and contain viruses.	Distributing a racist or obscene joke via e-mail.	Making a libellous or slanderous statement about a co-worker in an e-mail.

Section: PS 1103-sample

Technology	Core	Core/ Incidental	Incidental	Incidental/ Unacceptable	Unacceptable	Against Existing Policy	Illegal
Networked Computer on the Internet	Researching the latest development in your profession on the Internet.	An e-mail to a colleague deals with work and the schedule for your up-coming hockey tournament	Browsing a news site during the lunch hour to keep up with world events.	Subscribing to a newsgroup on a government internet account that is of a personal nature.	Downloading a beta version of a program off the Internet, and needing hours of IT support to get your computer re-started.	Buying and selling stocks at work on the Internet	Download, storing distributing and selling child pornography
Stand Alone Computer	Word Processing. Doing the budget.		Preparing a roster for your children's soccer team over the lunch hour.	Preparing a roster for your children's soccer team, tying up the computer when co-workers need to access it.	Crashing the computer by installing a graphics-intensive multi-player combat game.	Using the spreadsheet on the computer to analyse the performance of your stock portfolio.	Running a pirated version of a popular program on the computer

Note: These are examples only and not exhaustive or inclusive. Based on commonly used technology, departments will have their own instances of each category of use. Note also that employees are to cover costs incurred in personal incidental use such as long distance calls or photocopying - individual departmental policies may differ on how these costs are recovered.