Office of the
Saskatchewan Information
and Privacy Commissioner

HUMAN RESOURCE POLICY

2.1 IPC EXPECTATIONS
2.04 INFORMATION TECHNOLOGY RESOURCES

Purpose

To provide a policy framework that guides IPC employees to maximize the accountable and efficient use of IPC IT resources[1], and minimize risk to the integrity of OIPC Information systems.

To provide a policy framework that maintains the confidentiality of all case file material in accordance with *The Freedom of Information and Protection of Privacy Act* (FOIP) and the Oath of Office prescribed by section 44 of FOIP and section 54 of *The Health Information Protection Act* (HIPA).

The policy augments rather than replaces the Government Information Technology Acceptable Usage Policy (PS 1103).

Application

This policy applies to all employees of the Information and Protection of Privacy Commissioner (IPC) and anyone using IPC resources.

Confidentiality

All information stored using IPC IT resources belongs to the IPC and may be considered confidential. Appropriate steps must be taken to ensure that confidential information is protected.

Employees must have a requisite 'need-to-know' prior to accessing any information belonging to the IPC.

Employees of the OIPC must maintain confidentiality of all case file and other sensitive material in accordance with FOIP, HIPA and the Oath of Office prescribed by section 44 of FOIP.

[1] IT resources include but are not limited to Desktop computer and the software that is installed therein, laptops and the software that is installed therein, e-mail, internet, intranet, photocopier, fax machine, mobile phones, office telephones.

Background

The increasing use of information technology has, and continues to, fundamentally change the workplace. The internet, intranets, mobile devices, 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 OIPC to potential embarrassment and undermine public confidence and public sector confidence in the organization. The OIPC 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 OIPC IT resources is appropriate.

Policy

Employees of the IPC 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 IPC will periodically redefine and enhance these guidelines and policies.

IPC guidelines and policies which apply to:

- Oath of Office as prescribed by section 44 of the FOIP Act
- Confidentiality requirements prescribed by FOIP & HIPA
- OIPC Best Practices - Mobile Device Security; and
- OIPC Privacy Breach Guidelines

As well as Government of Saskatchewan policies which apply to:

- Harassment
- Performance improvement
- Conflict of interest; and
- Corrective discipline

Also applies when employees use the IPC IT infrastructure.

Information in the control of the IPC may be accessed only from equipment provided by the office. This may include, but is not limited to, IPC desktop computers, laptops and or mobile devices. Copying or forwarding such information is expressly prohibited.

No IPC case files, work product or part(s) thereof are to be removed, used or disclosed outside of the IPC for any purpose without the prior permission of the Commissioner, Director of Compliance or Director of Operations. The exception is the communication in the course of reviews and investigations with relevant government institutions and trustees by electronic means.

This policy augments, rather than replaces existing Public Service Commission policy.

Employees who violate this policy will be subject to disciplinary action.

There are three usage types for IPC IT resources: Core, Incidental, and Unacceptable.

Core uses are activities required to conduct the business of the IPC. They help to fulfill the mandate of the IPC. The IPC IT infrastructure primarily exists to facilitate core IPC purposes.

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

Unacceptable use impedes the work of others or needlessly squanders IT resources. It may unintentionally damage IT infrastructure, affect the ability of the IPC to deliver on its mandate, or generate additional costs.

It is unacceptable to:

- Use, copy or otherwise access IT resources without permission.
- Use the IPC IT infrastructure for activities that contravene the law, existing policies or regulations.
- Use the IPC IT infrastructure for any activities that are offensive or perceived to be offensive.
- Download or introduce data from an external source without proper authorization and without taking all available precautions such as ensuring it is virus free.
- Use any part of the IPC IT infrastructure for personal financial gain.
- Infringe copyright or proprietary rights.
- Permit unauthorized access to IPC IT resources.
- Create or knowingly propagate malicious, illegal or unauthorized software.
- Damage files, equipment, software, or data belonging to the IPC.
- Use, or attempt to use, unauthorized access methods or abilities.\
- Publish information of a derogatory or confidential nature relating to the OIPC.
- Cause, permit, or attempt any installation of hardware or software, destruction or modification of data or equipment without specific authorization.

The above list is not exhaustive.

While the OIPC does not prohibit limited incidental use of information technology for personal reasons outside of regular work hours (i.e., during coffee breaks or lunch break), users should recognize that the primary intention of providing this resource is to support the core work of the OIPC.

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

IT Resource Management

Only equipment purchased and managed by the IPC is permitted to access IPC IT resources; permission must be obtained from the Commissioner before any device or additional software is connected to any IPC network. In addition, relocation of IT resources must be done in coordination with the Director of Operations or the Administration branch of the IPC.

Monitoring

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

The unacceptable use of IPC information technology resources is an employment issue and will be dealt with through established human resources processes.

Acceptable Internet Use

Internet access is provided to employees to facilitate work related communication, research, and related activities. Employee access to the Internet is a privilege, not a right.

Employees must take steps to minimize the risks associated with Internet use. Discretion is required when choosing what websites to visit, and when using personally identifiable information on websites or forums. Sensitive information should not be transmitted via email or the Internet unless appropriate security precautions have been taken.

Access entails personal responsibility and employees are responsible for any activity carried out under their account. Use of the Internet is not anonymous; activity may be logged and monitored, and the IPC can easily be identified as the source of an email or visit to a website.

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
- Confidentiality requirements prescribed by FOIP & HIPA; and
- This policy

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 IPC. 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.

Unacceptable use of the Internet is when a user:

- 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.
- Bring the OIPC 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.
- Breaches the confidentiality requirements prescribed by FOIP and HIPA

Email created or sent on IPC systems is the property of the IPC and is not private employee communication, whether created or received. Employees should have no reasonable expectation of privacy in e-mail transmitted, received and stored on IPC IT systems.

Many employees access personal or work e-mail through web-based accounts hosted on sites such as Hot Mail or Netscape. Currently, this incidental use of IPC information technology infrastructure is permitted outside of normal working hours (i.e., coffee breaks, lunch break). However, web-based e-mail must be used cautiously.

Employees who access web-based e-mail with OIPC computers, mobile devices or networks are to follow the guidelines below.

- Web-based e-mail account names must be different from departmental 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 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, MUST 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.

Email is one of the leading sources of malicious software, including viruses and spyware, caution must be taken before clicking on any links or opening unexpected attachments. If you are suspicious that an e-mail may contain a virus, employees are to forward it to the Legislative Assembly helpdesk to have them check to see if it is virus infected (helpdesk@legassembly.sk.ca) prior to opening.

Unencrypted e-mail is not secure; employees have a responsibility to send only non-sensitive information via e-mail.

Whenever possible, personal e-mail should be sent via personal e-mail accounts.

Employees must create a signature file for official e-mail that is sent out from OIPC accounts. The text of the official signature file must list name, job title, organization as well as telephone and fax number. The signature file must also include a confidentiality notice which has been approved by the Commissioner.

The following confidentiality notice has been approved by the Commissioner:

Confidentiality Notice

This e-mail and any attachments are confidential and intended solely for the use of the individual to whom they are addressed. If you have received this e-mail in error please notify the sender. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute, copy, retain, use or modify this e-mail. Please notify the sender immediately by e-mail or by telephone at (306) 787-8350 if you have received this e-mail by mistake and delete this e-mail from your system. E-mail can be intercepted in transit or sent to the wrong address, so use secure means to communicate with us if you are concerned about confidentiality. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Passwords

Access to OIPC IT resources is enabled and controlled via user accounts. Employees are required to follow good security practices in the selection and use of passwords. Employees are responsible for their personal account information, including passwords.

All OIPC users must:

- Keep passwords confidential;
- Avoid keeping a record (e.g., paper, software file or hand-held device) of passwords;
- Change passwords whenever there is any indication of possible system or password compromise or at the very least every 12 months (avoid re-using or cycling old passwords);
- Select quality passwords which are at least six characters long and include a combination of numbers, letters, and/or symbols and which are:
    - Easy to remember;
    - Not based on anything somebody else could easily guess or obtain using person related information, e.g., names, telephone numbers, and dates of birth etc.;
    - Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
- Change temporary passwords at the first log-on;
- Not include passwords in any automated log-on process, e.g. stored in a macro or function key;
- Not share individual user passwords;
- Not use the same password for business and non-business purposes.

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. Using OIPC IT infrastructure to play games during work 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 multimedia games are also using IT resources in an unacceptable manner.

An incidental use would be an employee who spends a few minutes playing a game over the lunch hour, but employees are expected to use their common sense and good judgment. As always, “personal use on personal time” is a good rule to follow.

Data Storage

Staff should store all OIPC 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 OIPC business, on the network. The use of network storage devices will provide for recovery of such materials in the case of loss. Staff should not store copies of such materials on office computer hard drives, CD's, USB keys or other local or removable media unless necessary for their work. Storing materials on such devices exposes OIPC information and information systems to disclosure or unrecoverable loss.

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 the OIPC. In most cases participation is only appropriate as an individual. Whenever an employee engages in a public discussion through an OIPC account or is identified as being from the OIPC, the OIPC 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.

Authority

The Freedom of Information and Protection of Privacy Act, section 43.1

Influencing Sources

Legislative Assembly Service Policy 2.4
IPC Policy 2.07 Internal Social Media