



Department of the Premier  
Centre for e-Innovation

# Provincial Government of the Western Cape

## Centre for e-Innovation Policy Document

### **IT End User Policy**

**(Acceptable Use)**

Version: Version 1  
Date: 22 APRIL 2008


# Table of Contents

1	INTRODUCTION.....	4
1.1	Purpose.....	4
1.2	Definitions.....	5
2	REGULATORY FRAMEWORK.....	6
3	GUIDING PRINCIPLES.....	6
4	POLICY STATEMENT.....	7
4.1	General.....	7
4.2	Desktop Use.....	8
4.3	E-Mail.....	8
4.3.1	Acceptable Uses.....	8
4.3.2	Unacceptable Uses.....	9
4.3.3	Operational Guidelines.....	10
4.4	Internet.....	11
4.4.1	Acceptable Uses.....	11
4.4.2	Unacceptable Uses.....	11
5	PRIVACY GUIDELINES .....	13
6	COMPLIANCE WITH POLICY .....	14
6.1	Indemnity.....	14
7	SCOPE OF APPLICATION.....	14
8	RESPONSIBILITY.....	14
9	MONITORING AND CONTROL.....	14
10	POLICY EFFECTIVE DATE.....	15
11	APPENDIX A: EMAIL GUIDELINES.....	16
12	QUERIES.....	17

## Document Version Control

DATE	AUTHOR	VERSION NUMBER	REVISION DETAILS
22/04/2008	P&S	Version 1	Draft inputs finalised and approved.

## Approvals

JOB DESIGNATION	NAME	SIGNATURE	DATE
CHIEF INFORMATION OFFICER	Abe Freitas		10/4/2008

# **1 INTRODUCTION**

## ***1.1 Purpose***

The purpose of this policy is to ensure the proper use of Information Communication and Technology (ICT) assets of the Provincial Government of the Western Cape (PGWC). The policy applies to any ICT asset the PGWC has or may install in the future – including, but not limited to, e-mail, Internet, mobile data-cards and desktop computing. Users have a responsibility to use ICT assets in an efficient, effective, ethical and lawful manner.

Internet and e-mail Users must follow the same code of conduct expected in any other form of written or face-to-face business communication. The PGWC may supplement or modify this policy for Officials or other Users in certain roles.

## 1.2 Definitions

TERM	DEFINITION
Production Network	The "production network" is the network used in the daily business of the PGWC.
Modem	A modem is a device that modulates an analogue carrier signal to encode digital information. It is commonly used in connecting a computer to a telephone line.
Spam	Unauthorised and/or unsolicited electronic mass mailings.
Firewall	A firewall is an information technology (IT) security device which is configured to regulate network traffic reaching end user equipment (such as computers and servers).
Email	Electronic mail is a store and forward method of composing, sending, storing, and receiving messages over electronic communication systems.
Internet	The Internet is a worldwide, publicly accessible network of interconnected computer networks that transmit data using the standard Internet Protocol (IP).
Intranet	An intranet is a private computer network that uses Internet protocols, network connectivity to securely share part of an organisation's information or applications with its employees.
Extranet	An extranet is a private network that uses Internet protocols, network connectivity, and possibly the public telecommunication system to securely share part of an organisation's information or operations with suppliers, vendors, partners, customers or other businesses.
Internet Protocol (IP)	The Internet Protocol (IP) is a data-oriented protocol used for communicating data across a packet-switched network.
Official	All officers and employees (as defined in the Public Service Act, 1994) in the employ of the PGWC.
Contractor	All persons who are employed by third party companies or enterprises to do work at or for the PGWC on behalf of such companies or enterprises.
User	All persons, including but also in addition to Officials and Contractors, who use the Information Communication and Technology (ICT) assets of the PGWC.

## **2 REGULATORY FRAMEWORK**

- (a) Electronic Communications and Transactions Act, 2000 (Act 25 of 2002).
- (b) The Regulation of Interception of Communications and Provision of Communication-related Information Act 2002 (Act No. 70 of 2002).
- (c) Minimum Information Security Standards (MISS).
- (d) SABS ISO 17799 – best practice security standard.
- (e) Department of Public Service Administration (DPSA) regulation on Internet Access.

## **3 GUIDING PRINCIPLES**

The primary purpose of the Acceptable Use Policy is to protect the PGWC, Officials, Contractors, other spheres of government and other parties from illegal or damaging actions by individuals, whether deliberate or unintended. The primary guiding principle is that PGWC information technology assets should be used for PGWC business functions.

## 4 POLICY STATEMENT

### 4.1 General

- (a) The PGWC is governed by a broad range of legislation regulating telecommunications including, but not limited to, the Electronic Communications and Transactions Act, 2002, and the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, (the Interception Act). Users are bound by all relevant legislation and policies regulating telecommunications and electronic communications and undertake at all times to act in accordance with all relevant legislation and policies.
- (b) Users acknowledge that an "indirect communication" is defined in the Interception Act as:

"The transfer of information, including a message or any part of a message, whether (a) in the form of:

- (i) Speech, music or other sounds;
- (ii) Data;
- (iii) Text;
- (iv) Visual images, whether animated or not;
- (v) Signals; or
- (vi) Radio frequency, spectrum or

(b) in any other form or combination of forms; that is transmitted in whole or part by means of a postal service or a telecommunication system".

- (c) Users acknowledge that they have been granted access by the organisation to telecommunications information technology and resources, including e-mail and Internet access. The sole reason for providing such access to Users is to perform duties and responsibilities in accordance with their job function or other official purposes of the PGWC.
- (d) Users acknowledge that they have no expectation of privacy when utilising any telecommunications equipment and resources operated under the auspices of the PGWC and they grant permission to the PGWC to intercept, monitor, read, filter, block or otherwise act upon any electronic telecommunication, stored file or indirect communication which is or has been under their control, received by them or transmitted by them as contemplated in the Interception Act.

## **4.2 Desktop Use**

- (a) The device (Computer Desktop, Laptop) may not be connected to two or more networks simultaneously.
- (b) No modems may be connected to any devices that are attached to the PGWC's production network.
- (c) Users will be supplied with a username and password in order to access services on the production network of the PGWC.
- (d) Users must keep passwords secure and not share their account credentials. Users are responsible for the security of their passwords and accounts.
- (e) The device must be locked or logged off when unattended.
- (f) The device must be kept up to date with the latest anti-virus software and virus definitions and Operating System updates. This is achieved through the network log in process into the PGWC's production network.
- (g) Users shall not load any illegal or unapproved software onto the device.
- (h) Users acknowledge sole responsibility for any unauthorised or pirate(d) software found in their possession or on the systems and equipment allocated to or used by them.

## **4.3 E-Mail**

Electronic Mail usage is granted for the sole purpose of supporting organisational business activities. The PGWC supports the installation and usage only of approved email clients.

Usernames will be assigned by the PGWC (through the Centre for e-Innovation) and reflect internally mandated e-mail naming conventions.

### **4.3.1 Acceptable Uses**

- (a) Communicating in a professional manner.
- (b) Personal and private communications that are brief and do not interfere with work responsibilities.



- (c) Electronic messages are frequently inadequate in conveying mood and context. Users should carefully consider how the recipient might interpret a message before composing or sending the message.
- (d) Departmental mass internal e-mails, such as bulletins and information brochures, must be approved before dissemination. The dissemination process is communicated by the Centre for e-Innovation.

### **4.3.2 Unacceptable Uses**

- (a) Personal and private communication that interferes with work responsibilities.
- (b) Creating and exchanging messages that can be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or threatening.
- (c) Creating and exchanging information that is in violation of copyright or any other law. The PGWC is not responsible for use of e-mail that contravenes the law.
- (d) Opening file attachments from an untrustworthy source or with a suspicious or unexpected subject line.
- (e) Sending confidential information to unauthorized people or violating the Minimum Information Security Standards. Otherwise using e-mail in a way that increases the PGWC's legal and regulatory liability.
- (f) Communications that strain the PGWC network or other systems unduly, such as sending large files to large distribution lists.
- (g) Forwarding confidential business e-mail messages to personal accounts, because of unacceptable risks associated with privacy, security and compliance.
- (h) Using any e-mail system, other than the PGWC e-mail system, for PGWC-related communications.
- (i) Circulating chain letters and/or commercial offerings.
- (j) Circulating unprotected data and personally identifiable client/citizen data that would violate section 14 of the Constitution.
- (k) Promoting or publishing an User's political or religious views, operating a business or for any undertaking that offers personal gain.
- (l) Using the e-mail system for any purpose or in any manner that may prejudice the rights or interests of the PGWC or government in any other sphere.

### **4.3.3 Operational Guidelines**

- (a) The PGWC employs certain practices and procedures in order to maintain the health and efficiency of electronic messaging resources, to achieve business objectives and/or to meet various regulations. These practices and procedures are subject to change, as appropriate or required under the circumstances.
- (b) To deliver e-mail efficiently, message size must be less than 5 MB. Messages larger than 5 MB will be automatically blocked and users will be notified of non-delivery. Should this constitute a business hardship, users should contact the IT Helpdesk.
- (c) Users are encouraged to backup emails on their local drives. Individual online mailboxes will be cleaned up on the server on a regular basis. The mailbox clean-up happens on a weekly basis and items older than 260 days or larger than 8 MB are automatically deleted.

## **4.4 Internet**

Internet usage is granted for the sole purpose of supporting Organisational business activities necessary to carry out job functions. All Internet based transactions originating from within the PGWC's production network, are logged using the IP address of the workstation, the workstation host name, as well as the site visited and the time, for auditing and compliance purposes.

### **4.4.1 Acceptable Uses**

- (a) Accessing web based business applications and tools such as Logis and iPWIS.
- (b) Communication between Officials and non-Officials for business purposes.
- (c) Downloading software upgrades and patches.
- (d) Review of possible vendor web sites for product information.
- (e) Reference regulatory or technical information in line with the relevant the job description or official functions.
- (f) Accessing of Government Web Sites and portals.
- (g) Conducting research in line with relevant job description or official functions.

### **4.4.2 Unacceptable Uses**

Acquisition, storage, and dissemination of data that are illegal, pornographic, or which negatively depicts race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth is specifically prohibited.

The organisation also prohibits engaging in fraudulent activities, or knowingly disseminating defamatory materials.

Other activities that are strictly prohibited include, but are not limited to:

- (a) Accessing information that is not within the scope of the Official's work. This includes

unauthorised accessing and/ or reading of Organisational information, unauthorised access of personnel file information, and accessing information that is not needed for the proper execution of job functions.

- (b) Personal and private communication that interferes with work responsibilities.
- (c) Deliberate pointing or hyper-linking of the Organisation's Web sites to other Internet sites whose content may be inconsistent with or in violation of the aims or policies of the PGWC.
- (d) Any conduct that would constitute or encourage a criminal offence, lead to civil liability, or otherwise violates any regulations, directives or the common law.
- (e) The use, transmission, duplication, or voluntary receipt of material that infringes on the copyright, trademarks, trade secrets, or patent rights of any person or organisation. [Officials must accept that all materials on the Internet are copyrighted and/or patented unless specific notices expressly state otherwise].
- (f) Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls and the express permission from the relevant mandated parties.
- (g) Any form of on-line gambling and gaming.
- (h) The use of consumer grade Instant messaging clients.
- (i) Using the internet for any purpose or in any manner that may prejudice the rights or interests of the PGWC or government in any other sphere.

## 5 PRIVACY GUIDELINES

The PGWC maintains the right to monitor and review e-mail and Internet activity to ensure compliance with this policy, as well as to fulfil the PGWC's responsibilities in terms of legislation. Users have no expectation of privacy.

- (a) On termination or separation from the PGWC, access will be denied to e-mail and PGWC Internet, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.
- (b) Officials who leave the PGWC will have their mailbox disabled within one week of exiting the organisation.
- (c) The PGWC reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received. Intercepting, monitoring and reviewing of messages may be performed with the assistance of content filtering software, or by designated PGWC Officials.
- (d) The PGWC reserves the right to alter, re-route or block the delivery of e-mail messages as appropriate. This includes but is not limited to:
  - Rejecting, quarantining or removing attachments and/or malicious code from messages that may pose a threat to PGWC resources.
  - Discarding attachments, such as music, that are considered to be of little business value and involve a significant resource cost.
  - Rejecting or quarantining messages with suspicious content.
  - Rejecting or quarantining messages containing offensive language.
  - Re-routing messages with suspicious content to designated PGWC employees for manual review.
  - Appending legal disclaimers to messages.
- (e) Electronic messages are permissible as evidence in a court of law.
- (f) Any content created with the e-mail system is considered the intellectual property of the PGWC

## **6 COMPLIANCE WITH POLICY**

It is the responsibility of every User to take reasonable steps to ensure compliance with the conditions as set out in this policy document, and to guard against unacceptable use.

Users are deemed to have agreed to the policy when they plug a device onto the PGWC network or accept using equipment and resources owned by the PGWC.

Violation of this policy will lead to disciplinary action and/or removal of privileges, which may include an indefinite withdrawal or a suspension of service and privileges.

### **6.1 Indemnity**

By accepting this policy every User agrees to indemnify the PGWC against any civil claim brought and/or damages claimed by a third party against a Department or the PGWC as a direct or indirect result of non-compliance with the policy.

## **7 SCOPE OF APPLICATION**

This policy applies to Officials, Contractors and all other Users connected to the PGWC network and/or using PGWC equipment and resources. Wherever reference is made to Officials or Contractors or any other specific category of User in the policy it will be deemed to include, as far as possible, a reference to all other Users.

## **8 RESPONSIBILITY**

The Heads of Department will be responsible for the enforcement of this policy.

## **9 MONITORING AND CONTROL**

The Centre for e-Innovation will be responsible for monitoring compliance to this policy.

## **10 POLICY EFFECTIVE DATE**

1 JUNE 2008

## **11 APPENDIX A: EMAIL GUIDELINES**

*[Attached]*



## **12 QUERIES**

Queries and questions on this policy should be addressed to:

Policy and Strategy Directorate – Centre for e-Innovation

email: [ICTpolicy@pgwc.gov.za](mailto:ICTpolicy@pgwc.gov.za)