LIMPOPO

PROVINCIAL GOVERNMENT

REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
SPORT, ARTS AND CULTURE

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

TABLE OF CONTENTS

1. PURPOSE

a. To ensure that there is proper usage and maintenance of ICT equipment in the Department of Sport, Arts and Culture in line with policies and legislations of the Government of the Republic of South Africa.

2. OBJECTIVES

a. To provide fairness in the procurement and allocation of Desktops, Laptops and Printers.
b. Proper usage of the Email and Internet facilities in the Department.
c. Proper management and control of ICT equipments in the Department.

3. MANDATES

The ICT derives its work mandate from the following legal, policy and regulatory regime

- The Constitution of the Republic of South Africa Act 1996
- The State Information Technology Agency Act
- The SITA Amendment Act
- Promotion of Access to Information Act
- Public Service Act
- Public Finance Management Act
- National Archives Act
- Protection of Government Information Act
- Northern Province Tender Board Act
- Telecommunications Act
- Telecommunications Amendment Act
- Electronic Communications and Transactions Act
- Various other statutes
- Public Service Regulations
- Treasury Regulations
- White Paper on the Transformation of the Public Service (WPTPS)
- White Paper on the Transformation of Public Service Delivery (Batho Pele)
- Minimum Information Security Standards
- National Spatial Information Framework
- Government IT Policy Discussion Paper
- E-commerce Bill
- South African Information and Communication Technology Sector Development Framework
- ICASA Regulations
- Principles towards a Provincial Information Technology Policy, accepted by the Heads of Department in 1998

- Limpopo Growth and Development Strategy
- Public Infrastructure Investments Framework
- Northern Province Procurement Policy (NPT1)
- International Standards Organisation Directives
- Provincial Information Technology Committee (Northern Province Cabinet Decision 85 of 1995)
- ISO 17799 Standards
- EXCO Resolutions

4. ALLOCATION OF LAPTOPS, DESKTOPS AND PRINTERS

The Department of Sport, Arts and Culture is, as an employer, responsible for and is committed to providing members of its staff with a printer, a desktop personal computer and or a laptop for the performance of their duties, the execution of managerial instructions, and for communication purposes in and outside the department.

4.1 ALLOCATION OF DESKTOPS

A desktop personal computer is a standard piece of equipment, which should be provided to an employee whose nature of work needs the usage of a computer.

4.2 ALLOCATION OF LAPTOPS

a. Laptops are provided to the MEC, Head of Department, SMS, heads of district offices and managers.
b. Technical Staff, for example, information technology practitioners.
c. Members of staff who carry out secretarial duties for top management and similar other meetings may also be provided with laptops.

4.3 ALLOCATION OF PRINTERS

a. Printers shall be shared as one printer per office. Same applies for Senior Managers and Pa's.
b. Employees in the same office will share the printer, as it will be on the network.
c. Employees who occupy an office alone will be allocated a printer.

4.4 REQUISITION OF OTHER PERIPHERALS

A request has to be forwarded to GITO for other computer peripherals. E.g. scanners, headphones, projectors, web-cameras, special computers for the disabled.

4. 5 CUSTODIANSHIP

An employee to whom a laptop or a desktop has been allocated or provided, and who hereinafter is called user or the user or custodian, shall be responsible for the safety and custodianship of the desktop and or the laptop in and outside the office.

5. SECURITY

a. No person other than the custodian may have access to the desktop or laptop. The exception is the support technician, the contracted third party hardware maintenance and software support service provider, network and application system administrators.
b. It is the responsibility of the custodian to request identification from any of the listed personnel in 5.a above.
c. All laptops must be configured with a power-on password, which could only be unlocked by the owner or the manufacturer of the laptop.
d. The power-on password should be changed once every six months or anytime the custodian feels the password has been compromised.
e. The operating system has a password, which should be changed every two months. The operating system is configured to force a change of password every two months.
f. A password may not be repeated before a period of six months has elapsed.
g. A combination of digits and letters in both upper and lower cases must be used to coin a password.
h. Passwords should not be less than eight characters in strength.
i. Only laptops with the ISO/IEC 15408 standard shall be provided to custodians.
j. Employees who have been issued laptops shall ensure that his/her security access control identification card bears the departmental inventory number of the laptop.
k. The Security and Risk Management Unit shall ensure users comply with clause 5.j above when they enter or leave office premises.
l. No user shall be allowed to install any software of any kind without the knowledge of the GITO.
m. The rights to install software will only be given to the technicians, the system administrators and SITA.
n. The system administrator shall configure laptops or desktops to deny users access to reconfigure the desktop or laptop.
o. The server room must be locked at all times.
p. The door of the server room must have an electronic access.
q. GITO Manager and Risk and Security Management will know the access code to the server room.
r. SITA technicians will not have access to the server room without the knowledge of the GITO manager.
s. All computers and laptops will be installed with the Norton Antivirus, latest version.
t. All servers must have the Norton Antivirus and run on a live update.
u. A virus scan must be performed automatically for external storage devices before they can be accessed.

6. PROCEDURES AND PROCESSES FOR PROCUREMENT OF A LAPTOP, DESKTOP OR A PRINTER.

a. All requests should be directed to the GITO office through the supervisor of the requester / applicant.

b. A specification of any special software should accompany the request other than the standard software.
c. The GITO reserves the right to change the specification if needs be.
d. New equipment will only be purchased if there is a new employee, or the employee's old computer is beyond repaired.
e. The GITO office shall make a requisition to the procurement unit for the purchase of such requests.
f. A specification will be sent to service providers to supply quotations.
g. The relevant service provider with a reasonable quotation will be used to purchase such equipment in line with the PPPFA.
h. Stores will receive the purchased equipments.
i. The requisition officer will be contacted in order to verify that the equipment is in line with the specification before being recorded and coded by asset management.
j. The GITO will conduct desktops; laptops, printers and other computer peripherals audit analysis yearly in October.
k. GITO shall be allocated a budget for the payment of SLA's, software licensing, maintenance of equipment, purchasing of new equipment, i.e. printers, laptops, desktops, servers, software, computer peripherals, network cabling and connections.

7. MANAGEMENT OF THE LAPTOPS, DESKTOP AND PRINTERS AS ASSETS.

Upon departure from service in the Department, or upon vacation of an office or position by virtue of which a user had been allocated a laptop, a desktop and/or a printer, the following processes should be adhered to on returning the assets to the Asset Management division:

i. The user shall hand over such equipment and all its accessories to his or her supervisor. It is the user's responsibility to obtain an acknowledgement of receipt from the supervisor.
ii. The user's supervisor should deposit the equipment and its accessories with Asset Management within 7 days of receipt. The supervisor must obtain proof of deposit from Asset Management.
iii. The supervisor of the user shall be held personally liable for any loss incurred by the Department for the equipment that has not been deposited with Asset Management upon a departure of his or her subordinate.
iv. The user's supervisor shall, from the date of receipt of the equipment and its accessories, be responsible for the custodianship of the equipment until the date the equipment is entrusted to Asset Management.
v. No application or data may be deleted or removed from the hard drive of a desktop or laptop upon departure from office or upon vacation of a position.
vi. A supervisor of the user and Asset Management shall enlist the help of the GITO to ensure that the configuration of the laptop or desktop has not been violated, and the GITO shall issue a certificate or endorsement to this effect.
vii. At all times an internal asset database shall be maintained and updated.
viii. All equipment and accessories shall carry a barcode or an electronic tag.
ix. Only authorised technicians will be allowed to open equipment casing.

x. Movement of equipment from one office to another will be regulated as per Asset Management Policy.

8. SOFTWARE STANDARDS.

i. All laptops and desktops shall be configured and installed Microsoft Windows XP Professional Operating System as the Department's standard workstation operating system.
ii. All laptops and desktops shall be installed Microsoft Office 2003 as the standard office application package software.
iii. Acrobat Reader and WinZip shall be installed on all laptops and desktops.
iv. All users shall access the Internet using the Microsoft Internet Explorer browser, the latest version.
v. A standardised software will be utilized for the electronic messaging system for e-mail and other office application systems. E.g. leave management system, vehicle management system, time management system, bursary management system, administration system, and the intranet.
vi. All software packages shall be updated after every three (3) years.
vii. The Department will pay on yearly basis the licensing for software agreed in the Provincial Government IT Officers' Council or the Provincial IT Committee as provincial standards and in respect of which provincial contracts have been concluded or arranged by the Office of the Premier.
viii. No employee under any circumstance shall upload, download, and install any software without any authorisation from the GITO.
ix. All the software will be kept in a safe in the GITO's office.

9. MAINTENANCE AND SUPPORT SERVICES.

a. An SLA shall be signed with a certified service provider for repairs, maintenance and support of the equipment.
b. The SLA will be reviewed on a yearly basis in order to maintain service standards.
c. All SLA's will be submitted to Legal Services and Administration, Office of the Premier, before the Department can sign or commit itself to such agreements.

10. SERVERS

The Department shall have four servers, which will be allocated as follows:

- Mail server
- Proxy Server
- Back-up Server
- File Server

The Back-up server will backup documents, which are saved in the My Documents folder of each an every profile when logged on to the server. It is the responsibility of the users to always save their information in the My Documents folder and is connected to the network. Strict measures will be taken on the type of files that will be backed-up.

11. E-MAIL

11.1 Problem Statement

What this chapter seeks to address is informed by but not limited to the following problems: -

a) Organisations have spent millions of Rands litigating and settling lawsuits arising out of employee abuse and misuse of e-mail.
b) Confidential, Secret and other highly sensitive business information stored on computers have been stolen or inadvertently compromised by employees.
c) Unnecessary traffic on the network compromises network uptime and performance capacity.

The aim of this policy is to reduce, and possibly eliminate, some of these negative factors. Employees should be trained in using the system and be made aware of all the rules covered by this policy. Where applicable and possible, enforcement of the rules covered in this policy will be automated.

11.2 Access

Communications is a basic right entrenched in our constitution and therefore all employees are entitled access to e-mail.

The e-mail infrastructure administrators must be informed all the time when people join or leave the Department. New employees shall be assigned an e-mail address on the first day of commencing duty. All e-mail accounts of employees leaving the company shall be disabled within the last week of their notice period.

11.3 Configuration standards

The standard for configuring an e-mail address shall follow the universal naming convention of SurnameInitial@sac.limpopo.gov.za.

11.4 Password controls & precautionary measures.

Access to e-mail shall be password controlled. Employees are advised not to leave their workstations unattended to with their e-mail accounts live. All e-mail accounts will be locked automatically by the system after five (5) minutes of inactivity. All suspicious incidents should be reported immediately through the proper channels i.e. notify the administrator.

11.5 Usage

The use of e-mail shall be for professional purposes only. E-mail should only be used for business purposes, using terms, which are consistent with other forms of business communication. Personal usage will only be allowed on condition it does not infringe on other legal, democratic, human or moral rights nor interfere with the performance of work duties and responsibilities. Personal usage should be kept as minimum and as legal as possible.

11.6 Attachments

The attachment of data files to e-mail is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code. Care must be taken not to divulge Departmental confidential documents and other related secret documents. Users are encouraged to save the attachments on their hard drive and to delete the attachments from their emails in order not to overload the mail server.

11.7 Incoming mail

Incoming e-mail must be treated with the utmost care due to its inherent information security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code. All e-mails should be given a title that is commensurate to the content being distributed of the topic for discussion. All suspicious looking mail shall not be opened in all such instances; the administrator should be notified with immediate effect.

Unsolicited e-mail is to be treated with caution and not responded to. Employees shall ensure that information being forwarded by e-mail (especially attachments) is correctly addressed and only being sent to appropriate persons.

11.8 Prohibited usage

No explicit, illegal, harmful or derogatory content shall be sent through the departmental e-mail. Such will be treated as a criminal offence under including associated human rights legislations including the departmental internal code of conduct. All employees must be aware of the key aspects of copyright, designs and patents legislation. The use of departmental networks, tools and applications to infringe on copyright and patents is restricted. Employees will be held personally liable for any such infringements.

Users shall not use Departmental e-mail services to view, download, save, receive, or send material related to or including:

- Offensive content of any kind, including pornographic material.
- Promoting discrimination based on race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
- Threatening or violent behaviour.
- Illegal activities.
- Commercial messages.
- Messages of a religious, political, or racial nature.
- Gambling.
- Personal financial gain.
- Forwarding e-mail chain letters.
- Spamming e-mail accounts from Departmental e-mail services or Departmental machines.
- Material protected under copyright laws.

- Sending Departmental sensitive information by e-mail or over the Internet.
- Dispersing Departmental data to the public or clients without authorization.
- Opening files received without performing a virus scan.

Confidential documents shall not be sent to external parties unless necessary authority has been obtained. Such shall be done in an encrypted format. Unauthorised e-mail of top-secret and government confidential documents is strictly prohibited.

11.9 Bandwidth allocation

The maximum message sizes, including attachments, are as follows:

a)	Departmental Internal - Sending and receiving:	5.0 MB
b)	Departmental External (Internet) - sending:	2.0 MB
c)	Departmental External (Internet) - receiving:	3.5 MB

Additional memory will be allocated to the Senior Executives as well as other managers dealing with special projects and client interface. Any additional space required needs to be motivated for first and is to be documented and recorded accordingly.

Employees will not be declined the right to receive e-mail, purely on the basis of the fact that the mail is too big. All means necessary shall be taken to ensure that e-mails reach their intended destinations.

Message sizes should be as small as possible. The use of the built-in e-mail editor is advisable as external editors (e.g. MS Word) can create message files of almost double the size of the built-in editor. All attachments exceeding 1MB (e.g. Presentation graphics) should be compressed using a compression utility (e.g. PKZIP, WINZIP) prior to attaching and sending the message.

11.10 Data retention period

Data retention periods for e-mail must be established to meet legal and business requirements and must be adhered to by all staff. In order to maintain free space for new e-mails, prevent network/server congestion, as well as to improve processing speed, e-mails in the in-tray will be deleted every ninety days. Users must file e-mails (including attachments) in their respective folders/drives. The in tray should be kept as clean as possible.

11.11 Privacy and confidentiality

Notwithstanding the Departmental respect for employee's privacy in the workplace, the Department reserves the right to have access to all information created and stored on all systems. In this instance the Department reserves the right to inspect the contents of all e-mails at random. Please note that in the interest of security, prior warning will not be provided, however consent shall be priory obtained.

The Department shall strive to protect its messaging system against virus attacks. All mail received from or sent to the Internet will be subject to stringent virus control measures. In the event of any file being found to be virus-infected, it will be followed by a virus-alert message, which will be sent to the sender, recipient and the Departmental information security unit.

All Departmental e-mails shall carry a disclaimer clause, stating:

" The contents of this e-mail (attachments included), relating to official business of the Department, is the property of the Department of Sport, Arts and Culture and is therefore herewith protected

against any unauthorised use, deliberate or unintentional errors that might occur as a result of this transmission. The Department forfeits the right to ownership of any information that is not professional, this includes (but not limited to) personal e-mail, or opinions expressed by personnel who may or may not be the Department's employees. The person addressed in this e-mail is the intended recipient. Should this e-mail land in the hands of any third parties for whatever reason, such parties are requested not to disclose the contents of this e-mail. This error however is to be reported with immediate effect. This Department cannot ensure that this e-mail is free of any errors or viruses, interception or interference and will therefore not be held liable for any personal mail and/or opinions expressed herein."

11.12 Termination

E-Mail accounts will be eliminated a week prior to termination of duty. A frequent and open channel of communication should be kept between Human Resources Management and the system administrators.

12. INTERNET AND INTRANET

12.1 Access

All employees are entitled access to the Internet. Likewise all new employees shall be given access to the Internet on the first day of commencement of duty and all personnel that have left the Department shall be disabled immediately.

12.2 Illegal or harmful content

Employees shall not use the Department's systems to access or download material from the Internet, which is obscene, harmful, illegal, derogatory, inappropriate, offensive and or inflammatory, which will compromise or jeopardise the Department's and national security.

12.3 Intellectual property

Great care must be taken when downloading information and files from the Internet to safeguard against both infringement of intellectual property and copyright. In the event of no violation to intellectual property, information obtained from Internet sources should be verified before used. All information obtained on the Internet for research and other purposes should be acknowledged accordingly. Information contained in this site may only be used for non-commercial purposes.

12.4 Departmental Web content

Information presented at the Department's website is considered public information and may be distributed or copied freely unless identified as being subject to copyright protection. For all intended purposes, the Departmental website should be cited as the source of any information, photos and images. The contents of the Department's site may not be altered, reverse engineered, transmitted or broadcast without written permission.

12.5 Web development and administration.

Due to the significant risk of malicious intrusion from unauthorised external persons, the Departmental web page will be updated and developed by the Office of the Premier, as they are the owners of the provincial website. The CIO is responsible to update the Office of the Premier on

any changes that should be on the Department's web page. The Office of the Premier shall make detailed reports of activities and updates to the web page available for the CIO.

12.6 Hyperlinks

Care must be taken not to hyperlink web pages to the Department's web page without obtaining prior consent from the respective site owners. When visiting linked sites the user must refer to that linked site's individual terms of use and cannot rely on the terms of the Department's web page. These links are not intended to suggest that we endorse, recommend or favour any views expressed, or commercial products or services offered on these external sites.

12.7 Permitted usage

Internet use shall be restricted to business related purposes. Personal usage will only be allowed on condition that this does not infringe on other legal, democratic, human or moral rights nor interfere with the performance of work duties and responsibilities. Personal usage should be kept as minimum and as legal as possible. Users may use the Department's Internet services for personal improvement, outside of scheduled hours of work, if such use is consistent with professional conduct and is not for personal financial gain.

Users shall log off the Internet upon completion of a search/transaction. Users are advised to download materials from the Internet and process them in an offline environment as this proves to be cost efficient.

Staff authorised to make payment by credit card for goods ordered on the Internet are responsible for its safe and appropriate use.

12.8 Prohibited usage

Users shall not use the Department's Internet services to view, download, save, receive, or send material related to or including:

- Offensive content of any kind, including pornographic material.
- Promoting discrimination based on race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
- Threatening or violent behaviour.
- Illegal activities.
- Commercial messages.
- Messages of a religious, political, or racial nature.
- Gambling.
- Chat rooms and/or discussion groups.
- Personal financial gain.
- Forwarding e-mail chain letters.
- Spamming e-mail accounts from Department's e-mail services or Department's machines.
- Material protected under copyright laws.
- Sending business-sensitive information by e-mail or over the Internet.
- Dispersing information to the public without authorisation.
- Opening files received from the Internet without performing a virus scan.
- Tampering with your Department's handle in order to misrepresent yourself and the Department to others.

12.9 Privacy and confidentiality

Not withstanding the rights to privacy, in line with the Interception and Monitoring Act, the Department reserves the right to monitor online activity. Employees are advised to stay away from subscriptions, click wrap and shrink wrap contracts on the Internet as they often lead to spamming and all sorts of issues which compromise security, network performance and employee productivity.

12.10 Non-compliance

All personnel with Internet access (including e-mail) shall familiarise themselves and must ensure that they are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet (as stipulated in this policy) in addition to compliance with the Department's goals strategies, policies and code of conduct. Non-compliance to this policy will be subject to the normal internal disciplinary procedures or the South African criminal and justice system where applicable.

12.11 Liability

The Department will not assume legal liability for accuracy, completeness or usefulness of information disclosed on the web page and expressly disclaims liability for damages caused by computer viruses, which may consequently occur as a result of accessing the Department's web page and associated network infrastructure. All the Department's employees agree that they will not send submissions to the Department's web page that:

- are considered illegal,
- are for the purpose of spamming for political interests,
- restricts other users from using the web page,
- are abusive, obscene and pornographic,
- contains computer viruses,
- are intended for commercial purposes, contain marketing or promotional materials to solicit donations.

13. GLOSSARY

ACRONYM	DESCRIPTION
CIO	Chief Information Officer
Department	Department of Sport, Arts and Culture
GITO	Government IT Officer
Interception and Monitoring Act	Regulation of Interception of Communications and Provision of Communication-related Information Act, Act 70 of 2003
IT	Information Technology
MEC	Member of the Executive Council
SLA	Service Level Agreement
ICT	Information and Communication Technology

RECOMMENDED / ~~NOT RECOMMENDED~~

Recommended for approval

HEAD OF DEPARTMENT

28/07/05

DATE

APPROVED / ~~NOT APPROVED~~

MEC

22/08/05

DATE