

# NGAKA MODIRI MOLEMA DISTRICT MUNICIPALITY



# INFORMATION TECHNOLOGY POLICY

# INFORMATION TECHNOLOGY POLICY

## INTRODUCTION

The Ngaka Modiri Molema District Municipality is committed to allocate or provide Councillors, staff members and staff to Political parties with a computer and printing facilities to be able to perform their normal day to day duties. The Information Technology Policy is meant to ensure the usage, and security of this equipment is well managed and maintained, and that Information Technology Standards are adhered to.

## PURPOSE

The Information Technology policy guides the Ngaka Modiri Molema District Municipality on:

- Allocations of computers to Councillors and Staff
- Usage of software and IT equipment
- Physical and logical security (e.g. passwords, access to documents) to the equipment
- Standards to adhere to for maintenance of IT equipment.

## OBJECTIVES

- To specify allocations of computers in the Municipality
- To guide the IT section on how to deal with private equipment
- To guide users on the usage of the IT systems
- To guide users on the security of the IT equipment
- To specify standards that the Municipality adheres to

## SCOPE AND APPLICATION

This policy applies to all Councillors, staff and staff to political office bearers.

## LEGAL FRAMEWORK

Municipal Finance Management Act

Municipal Systems Act

State Information Technology Act

Promotion of Access to Information Act and Regulations

ICT Charter

## Roles and Responsibilities

- The IT section is responsible for implementing the directives issued by the Municipal Manager, and in ensuring that all ICT policies are adhered to.
- The Information Technology Manager may delegate any of his/her functions to others as is required for operational efficiency.

## **STAFF AND COUNCILLORS**

### **General**

#### **A. ALLOCATIONS FOR ADMINISTRATION STAFF AND COUNCILLORS**

- A.1. Desktop computers
- A.2. Laptops
- A.3. Printers
- A.4. Other peripheral devices
- A.5. Software
- A.6. Other software / programs / data

#### **B. COMPUTER USAGE**

- B.1. General
- B.2. Acceptable / Unacceptable usage
- B.3. Data management
- B.4. Viruses
- B.5. E-mail
- B.6. Internet
- B.7. Help Desk
- B.8. New users or changes to usernames

#### **C. COMPUTER SECURITY**

- C.1. Equipment
- C.2. Network access
- C.3. Data
- C.4. Antivirus and patch management
- C.5. Remote access
- C.6. Subscriptions
- C.7. Internet access
- C.8. Electronic banking and other such services

#### **D. STANDARDS**

#### **G. TRAINING**

## A. ALLOCATIONS FOR ADMINISTRATION STAFF AND COUNCILLORS

### A.1. Desktop computers

- All staff members will be provided with a Desktop computer and a printer if necessary to perform their duties
- All Personal Computers (computers) will be Intel and Microsoft Windows compatible, and will have Microsoft Office loaded.
- Allocations may change as needs and usage levels change, and as new equipment is purchased. However, no change of equipment will occur without the recommendation of IT Manager and approval of the Head of Department.
- The Municipality will **not** provide any person with a desktop computer or peripheral (including modem) for home use except per instruction and approval by the Municipal Manager
- No person may open a computer or carry out any hardware installations, repairs, modifications, etc. All such work must be carried out by the IT section.
- If any damage occurs with the desktop, the user needs to notify IT section in writing explaining the cause of damage and the sectional head and manager must acknowledge the receipt of the letter within 24 working hours.

### A.2. Laptop computers

- The Municipality will provide laptop computers to all staff on Management level as they are required to do some work out of their normal working hours.
- **The Municipality will provide laptop computers and mobile printers to all Councillors to perform their duties.**
- The Municipality will provide a limited number of laptop computers for staff members who according to their job requirements are required to use a laptop. The head/ manager of that section will be responsible for the allocation of the laptop.
- It is the responsibility of the user to make the necessary data backups of anything stored on the laptop hard-drive, as the IT section cannot guarantee recovery of lost data.
- If any damage (including virus infection or other software and hardware damage) occurs with the laptop, the user needs to notify IT section in writing explaining the cause of damage and the sectional head and manager must acknowledge the receipt of the letter within 24 working hours.
- Recovery of laptop when councillors or staff resigns rests with the Head of the Department or Executive Manager in the Office of the Mayor.

### A.3. Printers

- All staff and Councillors will have access to a printer. In the case where one could not be allocated his/her own printer him/her would be granted access to a network or shared printer.
- Specific printers will be allocated on the basis of the printing volumes and work context of the person, and may be re-assigned as required when necessary.
- Access to certain printers (i.e. high volume / colour printers) can be allowed by mutual consent between the sectional heads or managers.
- Allocations may change as needs and usage levels change, and as new equipment is purchased.
- No person may open a printer or carry out any hardware installations, repairs, modifications, etc. All such work must be carried out by the IT section. The only

exception is to replace an ink cartridge or correcting paper jams, which may be carried out by the staff or Councillor.

- The Municipality will provide ink and toner cartridges for official printers<sup>1</sup> only and will be installed by the IT section, and staff members knowledgeable to install them.
- If any damage occurs with the printer, the user needs to notify IT section in writing explaining the cause of damage and the sectional head and manager must acknowledge the receipt of the letter within 24 working hours

#### **A.4. Other peripheral devices**

- The Municipality will not provide any peripherals (such as scanners, memory sticks etc) to individual staff, Councillors or parties, unless it is specific in relation to perform their duties. Memory sticks will be provided to Councillors and Staff as a temporary backup solution.
- Replacement of Toners relating to the photocopiers will be the responsibility of the IT Section and the Service providers concerned.
- IT Section will be responsible to maintain and co-ordinate Telephone installation within the Municipality.
- Peripheral devices that are not frequently used will be acquired under the control of the IT Section

#### **A.5. Software**

- Copying of the Municipality's software by any person other than the IT section will not be allowed.
- No software supplied by the Municipality may be loaded onto any computer other than that of the Municipality.
- No person may copy, load or run any software that is not properly licensed.
- No person may load any software onto his or her computer. This function is only carried out by the IT section. This includes the downloading of any program files from the Internet.
- Each computer will be provided with a standard operating system, the standard "office" suite, e-mail, and web browser.
- The programs used by the Municipality may change from time-to-time as deemed necessary.

#### **A.6. Other software / programs / data**

- Should anyone receive a CD or a disk that provides a demo of software or any other item, it must be presented to the IT section, which will install them correctly for the user, and delete them when the usage has expired.
- The IT section may refuse to load any software should they believe that is not appropriate for the Municipality's IT systems, unless otherwise stated by Head of Department or Municipal Manager.

---

<sup>1</sup> Printers purchased by Ngaka Modiri Molema District Municipality

## **B. COMPUTER USAGE**

### **B.1. General**

- When appropriate, users (and/or groups of users) may be allocated a fixed amount of network disk space. This will only be imposed should the network disk space be abused.
- No hardware or software will be sold, lent or given to staff or Councillors, unless if Asset Management policy is adhered to regarding disposal of assets.
- When receiving a computer or any other peripheral equipment, the user is required to sign acknowledgement of receipt.

### **B.2. Acceptable / Unacceptable usage**

- No user may use a computer to send, access or download any inappropriate item, which may – *inter alia* – include:
  - B.2.i.a. Any item which carries any defamatory, discriminatory or obscene material;
  - B.2.i.b. Any item which carries any sexually explicit message, images, cartoons or jokes;
  - B.2.i.c. Any item which contain religious, racist or sexist slurs;
  - B.2.i.d. Any item which may be seen to be insulting, disruptive, and offensive to other people.
- No user may access, or attempt to access, whether physically or by other means, any equipment in order to gain access to material to which they do not have access as a normal part of their business at the Municipality.

### **B.3. Data management**

- All users should, as a matter of course, carry out all of their work on the **My Documents** Folder or H: drive, as these gets synchronized and backup centrally.
- The A: drive should only be used for small-scale backup purposes, and no disks obtained from outside the Municipality should ever be used.
- Stiffy / Floppy disks should never be used as a sole source for a copy of a file, as these disks are very unreliable, rather memory sticks should be used also.
- Should the IT section need to remove a user's computer (for repairs, to reallocate, etc), it is the responsibility of that user to ensure that they have made a copy of any data held on that computer. The IT section is not responsible for such a loss, and will not recover any such data that has been lost.

#### **B.4. Viruses**

- Anti-virus software will be provided by the Municipality to all computers connected to the network (including laptops issued with a network card).
- Any user who finds that the anti-virus software is either disabled or not functioning properly must immediately inform the IT section.
- If any user receives a virus from any source, they must immediately inform the IT section, and follow their instructions.
- If any user receives information relating to viruses, this should be forwarded to the IT section without delay and not copied to all users.

#### **B.5. E-mail**

- All members of staff and Councillors will be provided with access to E-mail.
- Every user will be provided with their own e-mail address, and have access to external e-mail communications.
- All users are expected to read their E-mail regularly - at least twice per day (first thing in the morning, and at lunch-time.).
- No users should send unnecessary messages ("please get ABC to contact me now") to large groups of people within the Municipality.
- No users should forward e-mail from outside that is "spam" – i.e. chain-letters, requests for help with worthy causes, etc.

B.5.i. Where a person wants to send a large file to a large number of users (i.e. anything containing graphics, or video, they should contact the IT Section to load the information on the Intranet, and the person may then send an e-mail with a link to that information.

B.5.ii. All users are expected to undertake house-keeping of their e-mail system on a regular basis. This involves deleting or archiving (as appropriate) messages that are no longer required. All attachments which need to be kept should be saved to disk, and the e-mail deleted. Users should also "Empty the deleted items folder" on a regular basis.

B.5.iii. The email system is not a system to archive important information or messages; this should be saved to the relevant disks or network shares. The IT section will not take responsibility for lost / archived or missing email messages.

B.5.iv. The IT contractor will maintain a strict limit on e-mail disk usage. If a user uses more than 200 MB of disk space, they will be sent a warning every time they send an e-mail. Once the limit of 250 MB is reached, they will be unable to send any mail until they have deleted (or archived) sufficient data to get below the 250 MB limit. However, it should be noted that even when the 250 MB limit is reached, all incoming mail will still be retained, up to 300MB so no information will be lost.

B.5.v. Disclaimers:

The following disclaimer will be added to all emails:

*The Ngaka Modiri Molema District Municipality retains all its intellectual property rights in any information contained in e-mail messages (or any attachments thereto) which relates to the official business of the NMMDM. Such information may be legally*

*privileged, is to be treated as confidential and the NMMDM will take legal steps against any unauthorized use.*

*The NMMDM does not take any responsibility for, or endorses any information which does not relate to its official business, including personal mail and/or opinions by senders who may or may not be employed by the NMMDM.*

*In the event that you receive a message not intended for you, we request that you notify the sender immediately, do not read, disclose or use the content in any way whatsoever and destroy/delete the message immediately.*

*While the NMMDM will take reasonable precautions, it cannot ensure that this e-mail will be free of errors, viruses, interception or interference therewith. The NMMDM does not, therefore, issue any guarantees or warranties in this regard and cannot be held liable for any loss or damages incurred by the recipient which have been caused by any of the above-mentioned factors.*

#### **B.6. Internet**

- B.6.i. All staff and Councillors with a computer connected to the network will be granted Internet access.

#### **B.7. Help Desk**

- B.7.i. Procedures to follow in submitting a service or helpdesk request: All requests for help/service(s) will be logged by the users using Help Desk System.

#### **B.8. New users or changes to usernames**

- B.8.i. No person may become a user of the Municipalities network unless requested by the HR department (for members of staff, Councillors).
- B.8.ii. If a person is transferred or fills another person's post (even in an acting capacity), no change will be effected by the IT section until the HR department requests it.
- B.8.iii. When a person leaves the employ of the Municipality, it is the responsibility of the HR department to inform the Technology Manager.
- B.8.iv. Where a person is dismissed or suspended, the HR department is responsible for ensuring that the Technology Manager and the IT section are informed without delay, so that the network access can be suspended.



## C. COMPUTER SECURITY

### C.1. Equipment

- C.1.i. The Server Room is out of bounds to everybody, with the exception of the IT Section employees.
- C.1.ii. Each user is responsible for the security of the computer (including screen, keyboard, mouse and any other peripheral such as a printer) provided by the Municipality to him or her.
- C.1.iii. Any item missing must be reported by the user to their Sectional Heads / Managers without delay, and followed up with a written communication outlining all the circumstances. A copy must be sent to the Technology Manager.

### C.2. Network access

- C.2.i. All users must always log onto a computer under their own username, and may not let anyone else work without that person logging in under his or her own username. If a person cannot log onto the computer under his or her own username, it means that, that person is not authorised to access the computer or is using the incorrect password.
- C.2.ii. All users are required to use a password to access their computer, and to change that password from time to time.
- C.2.iii. Any user who allows another user to obtain their password then becomes responsible for security breach and all actions taken by that user when using that password will be sole responsibility of the user and is taken as constituting a gross violation of this policy.
- C.2.iv. Users who share offices (and so cannot lock their office when leaving it) are expected to make use of the Password protection on their screen saver (**accessed via <control panel> <display> <screensaver> in Windows**). Other users are encouraged to use this facility as well.

### C.3. Data

- C.3.i. The Municipality recognises its need to maintain a high level of data security both internally and externally.
- C.3.ii. All computers in use in the Server Room will be protected by passwords, and all server consoles should be locked at all the time if not attended to.
- C.3.iii. All data on the file servers will be backed up to tape (refer to Backup policy).
- C.3.iv. All messages on the e-mail server will be backed up to tape regularly, but for practical reasons, no reliance should be placed on the ability of the IT section to recover old messages which have not been saved to disk.

- C.3.v. If users require a more secretive (but not necessarily secure) method of storing data, they may place a password on each file. However, should the password be lost, no-one can recover the file (certainly not the IT section)

#### **C.4. Antivirus and patch management**

- C.4.i Patch management and distribution is critical to resolve known security vulnerabilities and stability issues in Microsoft Windows operating systems and desktop applications. Up to date antivirus packages are just as important to protect the Municipalities information against malicious attacks.
- C.4.ii The Municipality has put in place an antivirus strategy with a centralized update facility. All desktops and laptops will have the antivirus client installed on their computers.
- C.4.iii However it still remains the responsibility of the user to make sure that their antivirus packages are up to date and if not, to contact the IT section immediately.
- C.4.iv The Municipality's IT section will distribute patches for all operating systems and office applications centrally via the network. However it is the responsibility of each user to make sure that the necessary patches are downloaded and installed.

#### **C.5. Remote access**

- C.5.i. Councillors and authorised staff will be permitted to connect through the remote access connection.
- C.5.ii. Until further notice, this access will be limited to mail services.
- C.5.iii. If problems occur on a computer being used for remote connection, it is the responsibility of the user to bring the PC into the Municipality for the problem to be analysed there. No support will be given to computers outside of the Municipality building. The Municipality will accept no responsibility for any damage done to the computer or information stored, either during transit or when being worked on.

#### **C.6. Subscriptions**

- C.6.i. Subscriptions to online services are limited only to services that will enhance and promote the business of the Municipality.

#### **C.7. Electronic Banking and other such services**

- C.7.i. This is permitted to all users but the Municipality will not be held liable for any activities pertaining to these services.
- C.7.ii. This privilege may be revoked if it found that its use is impacting negatively on the performance of the employee.

**D. STANDARDS**

- D.1. Wherever practical, all software should be off-the-shelf.
- D.2. The Network Servers will run under the MS NT operating system.
- D.3. Workstations will run under the MS Windows XP/Vista operating system
- D.4. Wherever practical, all software applications shall be Microsoft, including:
  - (a) Office XP, including
    - (i) MS Word for word-processing;
    - (ii) MS Excel for spreadsheets;
    - (iii) MS PowerPoint for presentations; and
  - (b) MS Exchange / MS Outlook for E-mail / office scheduling

**E. TRAINING**

All IT related training will be handled as per the existing Human Resource policies. The IT section will assist in the identification of IT related training needs, but will not co-ordinate the training as this function resides in the Human Resource.