WATERBERG DISTRICT MUNICIPALITY

INFORMATION TECHNOLOGY POLICY

1. **Introduction**

It is the responsibility of the Information Technology Division within the Corporate Services Department to ensure that policy, procedures and standards regarding computer-related items are defined and adhered to. This document will cover the procedures for Computer Services related functions as well as the policies regarding the standards for both hardware and software. The policy will be of a dynamic nature and therefore every effort will be made to keep this document up to date.

2. **Purpose, Scope and Applicability**

The purpose of the Information Technology Users policy of Waterberg District Municipality is to ensure consistent and coherent direction and control (Governance). People using IT policy must use good judgment in the implementation, configuration and usage thereof. This document sets out the policy to which computerization of the municipality will take place. All officials involved in the computerization of the functions of the municipality should adhere to this policy. The strategy is to consolidate current operations, to become an advisor on and an executor of the various program needs. To position Information Technology within the municipality so that it can effectively be used to improve "Service Delivery", and to ensure that Information Technology is capable of moving into the electronic information age. This means, "Empowering the Municipality to optimize service delivery to its client through the effective application of state of the art Information Technology."

Information Technology must always strive to deliver system that address the business needs and a business or enterprise approach must be followed to obtain this vision. We must look beyond our current systems and always ask the question on how can we improve our system delivery and support functions.

Problems must be seen as challenges. To implement 21st century technology, bold steps and a strategic management approach must be followed to break down resistance and fear of changes in the implementation of new hardware and software (especially the Munsoft Financial System).

Business and Information Technology fusion must be maintained when new technologies are implemented. Business refers to the Division of Information Technology as a whole, but also refers to other department and their divisions within the municipality as well as SITA, Local Municipalities, National and Provincial Local Government Departments, State Owned Entities (SOE), the Private Sector and third parties that might be involved.
Business must have the dreams and Information Technology must strive to realize these dreams with the implementation of business driven applications that operate on efficient hardware.

The fact that Government institutions (Municipality) and the Information Technology requirements change, as well as changes in the technology, makes the IT Policy a dynamic documents that must be reviewed biannually. System must become more online and the Internet can be utilizing to improve service delivery to the public and other parties that might be involved.

2.1 Services

The Information Technology Division offer the following services:

- IT End Users Support (Hardware and Software).
- End User Training (Formal-classroom situation).
- End User Support Training (informal-telephonic or individual).
- Office round to check if system is used optimally.
- Liaise with outsourced service providers i.e. SITA, SALGA, Provincial and National Local Government department regarding all escalated problems.
- Backup services.
- Disaster recovery plan
- Procurement of all IT equipment and Computer rollout.
- Audit of computer equipment.
- Computer Consumables such as Mouse, Printer, Ink and cartridges, Storages Disk.
- Data Security.

3. **References**

This policy document shall be read in conjunction with the following Acts and Standards.

- The Constitution of the SA, Act 108 of 1996
- Municipal Finance Management Act 1 of 2004
- Local Government Municipal Structure 117 Act 0f 1998
- Local Government Municipal Systems Act 32 of 2000
- Minimum Information Security Standards (MISS). (The purpose of the MISS is to establish policy frameworks for general guidance of Information Technology practices to ensure that IT as strategic resource is utilized fully and cost effectively.
- The State Information Technology Agency (SITA) Act, as amended.
- Electronic Communication Transaction Act.
- The protection of Information 84 Act of 1982
- The promotion of Access to Information Act
- The National Archives Act 43 of 1996
- Information Security Policy: Securing Information in the digital Age (Draft)
- Fire brigade Act 99 of 1987

4. **Vision for IT**

The Information Technology Division shares its vision with the District at large of" Equitable distribution of resources, development catalyst and service delivery in a co-ordinated, inclusive and sustainable manner" by its motto of achieving "Increased productive and quality service delivery through efficient use Information Technology and Systems".

5. **Table of Contents**

The following policies are covered in this document:
IT Asset Management Policy

- E-mail and Internet Policy
- Information Security Policy
- Guidelines on the use of IT
- Procedure Manuals

6. Definition and Abbreviation of terms

Computer virus	A computer program or script that interferes with, or damages the normal operation of a computer or any installed software. Virus programs are designed to infect other computers by hiding within e-mails or executable programs.
Copyright	Copyright is designed primarily to protect an artist, publisher, or other owner against any unauthorized copying of his works, by reproducing the work in any material form, publishing it, performing it in public, filming it, broadcasting it, causing it to be distributed to subscribers, or making any adaptation of the work. A copyright supplies a copyright holder with a kind of monopoly over the created material, which assures him of both control over its use and the pecuniary benefits derived from it.
Municipality	Waterberg District Municipality
Prescripts	Regulations, instructions and directions.
Removable storage device	A removable disk on which data may be stored. Usually refers to the 3½-inch diskette. For the purpose of this policy this term includes any removable storage device fitted to a personal computer.
Personnel	includes employees/staff/officials employed permanently and temporarily as well as supplied by labour brokers or service-providers
Personal Computer	Computer Equipment being a Desktop or Laptop/Notebook assigned by **WDM** to personnel for business activities and official use.
CASCADING	Cascading is the term often given to the movement of PCs within

	an organisation
Download	Acquiring (getting) a file /data from internet
FTP	File Transfer Protocol, used for transferring data/files on the internet
Hyperlink	Automatic link to a URL
Personal Account	An account created on the computer for individual User for official usage
URL	Uniform Resource Locator, the address of a specific website
User	Authorised individual, making use of the Municipality IT Infrastructure
WDM	Waterberg District Municipality
DPLG	Department of Provincial and Local Government
DLGH	Department of Local Government and Housing of Limpopo
SITA	State Information Technology Agency
ITO	Information Technology Office, managed by the I.C.T Offiers.
IP	Intellectual Property
PC	Personal Computer
ISP	Internet Service Provider
CD	Compact Disk
GIS	Geographical Information Systems
SITA	State Information Technology Agency
IARF	Information Asset Release Form
WWW	World Wide Web
GIS	Geographical Information Systems

INFORMATION TECHNOLOGY ASSET MANAGEMENT POLICY

1. Introduction

IT assets and equipment are a crucial element to every business environment, they provide for efficiency in day-to-day tasks and the communication needs of an organization. Despite their usefulness, IT assets can expose the Municipality to several risks. This policy on the use of IT Assets aims to provide for effective control, management and maintenance of the IT equipment.

2. Purpose

The purpose of this policy is to regulate usage of IT Assets so that the Municipality:

- effectively controls the economic interest of computer software and hardware resources
- reduces total cost of ownership (TCO)
- Increases the return on IT infrastructure investment
- maintains an accurate and current inventory of the Municipality's IT assets
- encourages proper and efficient use of **WDM** IT assets
- minimizes loss of, and damage to, computer equipment, software and data
- is protected from possible legal difficulties due to computer usage
- is productive, by limiting personal use to reasonable levels.

3. Scope of the Policy

This policy is applicable to all permanent, contract and temporary personnel employed by the **WDM** who have been issued with a Municipality computer. In this policy *"personnel"* includes employees/staff/officials supplied by labour brokers or service-providers to the Municipality.

This policy refers to "users" as all computer users at the **WDM**, whether they are permanent, on contract or temporary employees.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose personnel use the Municipality's computers.

4. Policy Statement

4.1 COMPUTER SYSTEMS AND EQUIPMENT OWNERSHIP

All computer equipment, printers, software licenses, network and data that employees use at the Municipality shall at all times remain the property of the**WDM**.

If an employee has been issued with computer equipment by the ITO on behalf of the **WDM**, by signing a declaration form such an employee accepts full responsibility for the safekeeping and proper use of said equipment and accessories while in his/her possession.

4.2 ACQUISITION AND ALLOCATION OF COMPUTER EQUIPMENT

At the request of the employee's manager, accompanied by a signed appropriate Application for IT Equipment Form, computer equipment may be procured and an employee may have access to computer-based services. These are provided to assist the employee to fulfill his/her official duties and/or business activities. The ITO sets the qualifying criteria.

New equipment will be procured only if current equipment does not comply with the minimum standards set for the computer equipment. Printers are allocated in the same way but employees will be expected to share printers with other personnel.

In cases where an employee requires the allocation of non-standard equipment or software to fulfill their duties effectively, the employee's senior manager or head of the section must make a recommendation in the form of a motivated submission to the ITO. The submission must include the details and cost of the software or equipment required.

4.3 MANAGEMENT OF IT EQUIPMENT

The ITO is responsible for the management of IT Assets and the asset Life Cycle management processes including standards, acquisition management and long range planning. Authority to acquire IT assets is held by the IT.

4.4 STANDARDS

4.4.1 The ITO will specify the standard issue personal computer

To make for cost-effective use of equipment and software, the Municipality will standardize on a core set of software and hardware product requirements. The specifications will be set and revised from time to time by the ITO. The standards will cover the following:

- Minimum specifications for current desktop computers. Users may only request new computers if their current computers do not comply with the minimum specifications set by the ITO. (Annexure A)
- Hardware specifications for standard issue desktop computers, notebook computers and printers. Users will be issued with a computer that meets this standard. When the standard is raised, computers below the standard can be upgraded or replaced, if the computer is found to be inadequate by the ITO, it will be upgraded or replaced.
- Specifications for new desktop computers, notebook computers or printers. When the Municipality buys a new computer or printer, its specification will conform to this standard. The ITO will normally follow the standard set by the State Tender Board or SITA's Information Technology Acquisition center.
- Standard issue software set. A list of software that will be installed on all computers by default.
- Additional software set. A list of software that may be installed if needed to do the job. To control maintenance cost, no other software may be used without the written approval of both the user's Manager and the ITO.

4.4.2 Non-standard items will not be supported

The ITO supports a large number of products - both hardware and software. To keep costs down IT Support limits the product range it is willing to support and provide training for. If an employee uses software that falls outside this product range, the ITO cannot guarantee support for such a product. All reasonable requests will be considered and where the majority of employees require a non-standard product, the ITO will consider adding it to the list of items supported.

4.4.3 Allocation of personal computers as well as a laptop computer to employees

Employees are not entitled to both a laptop computer as well as a desktop personal computer (unless authorized by their Head of Department and the ITO). An employee may not request that a laptop computer be procured, if such an employee is already in possession of a desktop personal computer and vice versa. If a person is in the possession of a personal computer and requires a laptop the equipment will be cascaded to next line personnel or be kept in the ITO storeroom. A written motivated submission stating reasons why the employee requires an additional laptop or personal computer shall be attached to the Standard Application form.

Submissions for the procurement of mobile/laptop computers to be issued on a pool type basis will be considered by the ITO if the motivation is adequate.

4.5 USAGE OF IT EQUIPMENT

4.5.1 Classification of Computer Users

Employees are classified into two categories according the nature of their work. Standard users are employees who only use standard applications installed on their personal computers. High-level users are employees who use standard software and additional applications used in their divisions e.g. Financial Systems.

4.5.2 Use of computer equipment for official purposes

Computer equipment is issued to employees for official duties and for Municipality's business or activities sponsored or authorized by the Municipality.

4.5.3 Use of computer equipment for non-official purposes

Occasional and brief use of computer equipment by employees for personal use is allowed, but not encouraged, subject to the following restrictions:

- Personal use should not hinder productivity.
- Only incidental amounts of employee time, time periods comparable to reasonable breaks during the day, should be used to attend to personal matters.
- Personal use should not cause the Municipality to incur a direct cost in addition to the general overhead.
- Employees may not install or use software that does not support official business or activities sponsored by the Municipality, for example games, screensavers, screen utilities, movies, songs not on original CD, pictures, etc.
- Personal use shall comply with all other terms of this policy.

4.5.4 Storing of material on computer equipment

Users should take care not to expose the Municipality and its employees to materials or information that could be considered offensive. This includes words, images of any kind and recorded sounds (audio). If someone else accidentally sees material stored by an employee, the employee could face a charge of harassment. Regular harassment can create a hostile working environment for co-workers.

Storing of the following material is expressly prohibited:

- Discriminatory, intolerant or derogatory matter based on race, religion, gender, age, ethnic or social origin, sexual orientation, disability, physical condition, HIV status, conscience, belief, political opinion, culture, language or birth.
- Any form of violence, pornography, explicit nudity, sexual acts, gross depictions, religious content deemed inappropriate by other religious groups, militant or extremist material.

4.5.5 Computer Equipment should be switched off after hours

Unless computer equipment needs to run after hours, an employee shall switch off the equipment at the end of each working day. How? Click Start, Shutdown and OK) then Switch off the on/off button on your monitor). If an employee's computer is not logged out it is a security breach to the Municipality. Switching off of computer equipment is considered best practice to reduce the risk of fire, save energy and ensure that any documents that employees have worked on are properly closed and ready for backup.

4.5.6 Computer Equipment should be logged into the network

The Municipality provides its computer users with access to networked services. It also maintains computers remotely via the network. Computers that are not logged onto the network cannot access networked services and cannot be maintained remotely. For this reason, employees may not use computer equipment without first logging into the Municipality network. Employees must remain logged in when using computers. A support account will be created automatically on each workstation for support purposes.

Employees must lock their workstations when they are out of the office, the workstation must also have a screensaver with a password that will be activated automatically after a few minutes.

4.5.7 Work should be saved on the central space allocated per division on the network

Employees are advised to save all computer-based work they produce on the central space allocated to their division on the network. The Municipality provides employees with network-based storage. Each user has a home drive on the network. It does however have a space restriction of 200Mb per user (unless otherwise authorized by the ITO). If a failure does occur, work stored on the network can usually be recovered from a back up. If employees are producing work that needs to be shared, the employees should ask the Network Controller to set up a shared folder on the network.

Employees may not save files on any of the network drives that are unrelated to Municipality business. Any private or personal files should be saved by employees on a removable diskette and not on the local drive.

4.6 INSTALLATION OF HARDWARE AND SOFTWARE

4.6.1 Only authorized support staff may install or copy software programs

To avoid breaking the law, the Municipality needs to control carefully the software licenses it owns. For this reason:

- Only authorized support personnel may install or upgrade software on a Municipality computer. A valid license must be allocated to each installation.
- Only authorized support staff may copy computer programs. A program may be copied only if allowed by the license agreement, and then only for official purposes. A user may be held personally liable for any damages, and legal costs, if he or she copies software illegally.
- Maintaining central control over licenses and installations also protects the users from unknowingly breaking the law.

4.6.2 Personal software may be provided, within limits

There are circumstances where users will be allowed to provide their own software, or software licensed to a service provider. In this case, the employee must provide documentary proof that the employee holds a valid license before the software will be installed. The Municipality has the right to hold the license until the software is removed. The Municipality will not replace a license if it is lost, nor offer compensation.

Only authorized support staff may install the user-provided software programs.

4.6.3 Software written by the WDM

The **WDM** will normally own the copyright for software written "in-house", by the Municipality. Such software may be used within the Municipality without a license. But, users must still have these programs installed by authorized support staff.

Employees are still committing an offence if they copy, for non-official use, software owned by the Municipality.

4.6.4 Use and Storage of unlicensed software

Unlicensed software is illegal and not allowed on any computer in the Municipality. The Copyright Act 98 of 1978 protects intellectual property against theft. If an employee uses software without a license, the employee may be found guilty of a criminal offence. The author of the software may also seek civil damages. If an employee knows or suspects that software on computer equipment is unlicensed, the employee must contact the ITO. If employees infringe on applicable licensing and copyright laws the Municipality will hold such employees liable for criminal or civil action.

4.6.5 Responsibility for offensive material

Offensive material may have been stored on an employees' computer by another user - either accidentally or in violation of Municipality policy. An employee may accidentally view this material. The **WDM** is not responsible for material viewed in this manner. An employee uses his/her computer at their own risk. If an employee

discovers any offensive material on his/her computer, or on the network, the employee should report it to the ITO.

4.6.6 Managers may monitor software use by staff

The Municipality has a right, but not a duty, to monitor any aspect of its computer system, including use of the software on its computers. Monitoring is justified by the need to apply this policy and to measure software usage for licensing purposes. Managers may monitor a particular software program, use by certain individuals or use by their staff as a whole.

4.7 USE OF WDM RESOURCES

Employees shall take care to use all computer equipment and resources in a responsible, ethical and lawful manner. No employee should waste computer resources or unfairly prevent others from the use of such resources.

Employees may **not** use the Municipality's computer facilities to:

- Play games or run other entertainment software, unless the ITO has provided this software as standard software.
- Save files containing images, music, sound or video onto Municipality servers, unless they are for official purposes. In such official cases an employee computer's local hard disk shall be used to save such material. This is usually the C: drive.
- Make or store illegal copies of material protected by copyright. This includes software programs and publications, in whole or in part.
- Back up their local hard drives onto Municipality servers.
- Print large documents if there is a viable on-screen alternative.

4.8 MAINTENANCE OF COMPUTER EQUIPMENT

4.8.1 Employees have a duty of care for the equipment issued to him/her

Employees are expected to take good care of public property issued to them. This is particularly relevant to staff who use portable equipment such as notebook computers and flash disk. Employees must take reasonable precautions against loss and damage.

4.8.2 Lending of Computer Equipment

Employees who borrow or lend equipment (pool laptops or mobile printers) from IT for usage should fill in the IARF and specify when will they return the equipment. It is the responsibility of the employee to make sure the equipment is kept safely and returned to IT in good order.

4.8.3 Employees must obtain an Equipment removal control form before taking equipment off-site

Employees may need to take equipment (printers or pool laptops) off Municipality premises, either to work at home or at another site. Employees must obtain equipment removal control forms from the ITO. (If equipment needs to be removed outside of normal working hours the employees' Program Manager may authorize the removal. The ITO must be notified if this occurs). The form must indicate the employees' name as well as the description and serial numbers of equipment to be removed. The form must also indicate an expiry or return date. Employees issued with laptops are automatically given the permission to take it home but should fill in the equipment removal control form once.

4.8.4 Employees may not install, move, and tamper with computer equipment

Only authorized support personnel may move, upgrade or repair computer equipment. Employees may not remove, install or tamper with any internal component of a computer or the equipment that may be attached to it (e.g. printer). Employees may not move computer equipment to another room, or site - unless it is specifically designed to be carried around (e.g. notebook computers). Employees may not swap equipment with other users. Moving or swapping equipment will create inconsistencies in the asset register. Employees should contact the ITO, who will arrange for the equipment to be moved or installed for them.

Employees need to complete IARF forms for any computer equipment that is removed from their control. This includes equipment removed for upgrade or repair.

Users may open a printer to remove or replace paper as well as toner or print cartridge.

4.8.5 Upgrade of Computer Equipment

New equipment will be bought only if current equipment does not comply with the minimum standards set for the computer equipment.

- The end user initiates the process of approval and procurement of new equipment, replacing the outdated equipment as described in Acquisition, Delivery and Installation Process of Life Cycle Management – Stage 1.
- The end user completes an IARF by which the responsibility/accountability for the old equipment is transferred to IT for safekeeping and/or testing and write – off. This will then follow the Termination Process of Life Cycle Management – Stage 3.
- The end user hands the original IARF to the ITO while he retains a copy. An IARF must be completed and signed by the user and the ITO to transfer the equipment to IT for testing. A copy will be kept by the user.
- The IT Technician will change the status of the equipment "To be Tested" on the IT asset register.

4.8.6 Lost or Stolen Equipment

If an employee loses or damages equipment, software or data that belongs to the **WDM**, the employee must promptly report in writing to the Head of Department and the ITO. In the case of theft or suspected theft, the employee must also report the loss to the South African Police Service within 24 hours of the loss being discovered.

- In terms of the Municipality practices and policies, the user must provide the ITO with the following information:
    - Serial number of the IT Asset that was stolen or lost.
    - Case reference number of the South African Police Service (SAPS).
    - Date it was stolen and a short description of what happened.
- The ITO will then change the Status of the item/s to "Stolen/Damaged".

4.8.7 Damage of Computer Equipment

- Computer equipment that has been damaged willfully or as a consequence of negligence must be transferred between an end user and an ITO by means of an IARF**.**
- The end user will complete the IARF and supply the ITO with a copy, which will provide a detailed report that will also serve as information to support a decision to be taken on the liability for the repair costs of damaged equipment.
- After the repair costs and the circumstances have been established the end user will be notified of the outcome. As in the case of stolen assets the ITO must be notified.
- The ITO will update the IT Asset Register of the outcome of the decision to replace or to repair the damaged equipment.

4.8.8 Employees may have to pay for lost, damaged or stolen equipment

If an item is lost, damaged or stolen while it was under an employees control or responsibility, the **WDM** will not normally ask the employee to pay for it. But, employees may lose this cover if they fail to follow treasury regulations or standing instructions. The main elements are summarized here, but this summary does not replace the original prescripts which will be used to deal with any loss.

An employee may lose liability cover against loss if the employee:

- was not conducting official business when the loss occurred;
- was under the influence of alcohol or drugs when the loss occurred;
- had not been issued with a permit to take the item off Municipality premises;
- did not obtain a receipt for equipment voluntarily surrendered by an employee;
- acted recklessly or negligently;
- intentionally caused the damage; or
- ignored any standing instructions i.e. Finance procedures.

4.9 MOVEMENT OR CHANGE OF LOCATION OF COMPUTER EQUIPMENT WITHIN THE WDM

End users, who intend to move computer equipment will complete the standard IARF, keep a copy and forward the original to the IT Technician before the equipment can be moved. The Technician will do a physical verification between the IARF, the equipment and the IT asset register, before as well as after the move of location. The IT Asset Register will be amended with the end user's new physical location and contact details.

4.9.1 Computer equipment of Officials who resign

- When an official resigns he/she must return IT Assets in good working condition.
- It is expected from all end users to sign off their responsibilities with regard to all the computer equipment that has been issued and entrusted to them when they leave by means of the Municipality Employee Exit Checklist that s/he obtains from the Human Resource Municipality of the **WDM**.
- The ITO will check if the content on the form completed by the user corresponds with the IT asset register and the physical IT assets.
- The user must also complete the IARF and provide it to the ITO for the Asset register database to be updated.

5. Application of this policy

The ITO is responsible for the implementation and enforcement of this Policy. The Policy will be applied in several ways:

- Where technology allows, the policy will be enforced automatically. Management reports will highlight possible violations. These will be investigated to identify actual violations. The offender's manager will take disciplinary action in line with Municipality policy.
- Users may self-police the policy by reporting any violations via the grievance procedure.
- The ITO may issue a specific instruction.

5.1 EMPLOYEES MAY FACE DISCIPLINARY ACTION IF THEY VIOLATE THIS POLICY

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the Memorandum of Understanding on Conduct of Service 1994. or any collective agreement or statutory provision that replaces this. Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

5.2 MANAGERS ARE ACCOUNTABLE FOR COMPUTER USAGE BY THEIR STAFF

Managers should ensure that all their computer using staff, whether temporary, permanent or contracts are made aware of the contents of this policy. An employee is accountable for his/her usage of the Internet service and other computer related services.

6. **Commencement and Revision**

This policy takes effect on "DATE" and will be reviewed annually. The policy may be amended from time to time. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on the municipality by way of e-mail or memo.

7. **Annexures**

7.1 **ANNEXURE A - Minimum specifications of present equipment in WDM**

Desktop Computer		**Laptop Computer**	**Software installed**
CPU	Pentium III 550MMX	Pentium III	Application Software (MS Office XP Professional)
RAM	128Mb (Memory)	128 Mb Memory	Document Management System (Munadmin)
			Geographic Information System (GIS)
HDD	20Gig	10Gig	Norton Antivirus Corporate Edition
SCREEN	14 "		Operating System (Ms Windows XP Professional)
			Finance System
			Payroll System
			Project Management Software

7.3 ANNEXURE C – Declaration Form

DECLARATION

I, the undersigned, acknowledge that I am an employee with the WDM and hereby declare:

1. CONTACT PARTICULARS

Title		**Initials**		**Surname**	

Employee No		**Tel / Ext No**		**Cell Phone No**	

Division		**Directorate**	

Office Number and Building (e.g. 2 Mark Stret)	

2. The **Municipality,** through the ITO, is the rightful owner of the following computer equipment which has been issued to me, as listed hereunder, and for which I am responsible as a **User** with the following **User ID Number:** ……

Asset Category	**Make**	**Model**	**Serial No**	**Item No**
CPU / Desktop				
VGA Screen				
Printer ***(Complete if applicable)***				
Scanner ***(Complete if applicable)***				
Notebook/Laptop ***(Complete if applicable)***				

Other equipment *(Mark with an X)*	**Keyboard**	**Yes**	**No**	**Mouse**	**Yes**	**No**	**Speakers**	**Yes**	**No**

Additional Software		

3. As a registered User I am aware of and undertake:

(a) To take reasonable care to prevent the willful or negligent loss of or damage to the equipment,

The following factors should also be considered:

- In the event of damage to the equipment at any time while it is in the **user's** possession, the **user** agrees to inform the **ITO** immediately.
- The **User** agrees to pay the cost of repairs of all damage to the **equipment** caused by the **user's** lack of due care, negligence, or misuse.

(b) To make use of the Municipality Support Services of the ITO for the maintenance of the **equipment**,

(c) To adhere to all the Municipality IT Asset and Inventory Control Procedures, the Security Division's policies and measures in this regard, as well as the Financial Circulars pertaining to the loss of or willful damage to equipment.

(d) To notify the ITO as per **IT ASSET RELEASE FORM** of my intention to move the **equipment** should it become necessary for the performance of my duties?

(e) To notify the HR and ITO in writing of my resignation and to return all of the **equipment** listed in terms of this Declaration to the ITO.

The following factor should also be considered:

- Failure of the **user** to return the **equipment** may result in the **WDM** taking legal action to recover said **equipment** and recover any damage thereto, or recover the depreciated value thereof, at their sole discretion.

4. With reference to the Support, Maintenance and IT Asset Control policies and the procedures and standards of **equipment** of the **Municipality**, the **User** also accepts:

(a) That all **equipment** will be configured and maintained by the **Municipality** only.

(b) That **equipment** may not to be exchanged between **Users** or workstations.

Signed at …… on …… day of …… 200…….

…… ……

USER **IT OFFICE**

INITIALS, SURNAME AND POSITION IN PRINT:

……

……

WITNESS (User's Manager

INITIALS, SURNAME:

……

…… **DATE:** ……

FOR USE BY ITO

The Asset Register has been updated. YES NO

Date …….

Name in print …… Signature ……

7.4 ANNEXURE D - IT Asset Release Form

NOTIFICATION FOR REMOVAL/TRANSFER OF IT ASSETS

[This form must be utilized as the only standard document for the movement of IT assets. To be completed and signed by computer users when transfers of assets occurs between locations and between users, and during the resignation of personnel]

FROM		TO	
1. Employee (user) [e.g. Mr. Lesia Sibiya]		**2. Employee (user)** [e.g. Ms. Lisa Johnson]	
3. Office & Building [e.g Mark Street]		**4. Office & Building** [e.g.Mark Street]	
5.Telephone Number		**6. Telephone Number**	
7. Division & Directorate [e.g. ITO]		**8. Division & Directorate** [e.g. FBS]	

Category (eg CPU)	**Make** (eg Mecer)	**Model** (eg, Premium X)	**Serial no** (By manufacturer)	**WDM no** (Permanent marker no)

Transfer of the above listed IT assets between employees / users:

Released (signed off) by: …….. Date: ……

Received by: …….. Date: ……

For updating of the above records on the IT asset register, please submit this form to the ITO

FOR USE BY ITO ONLY

The Asset Register has been updated. YES NO

Date ……

Name in print ……

Signature ……

E-MAIL AND INTERNET POLICY

1. Introduction

Electronic mail refers to the electronic transfer of information typically in the form of electronic messages, memoranda, and attached documents from a sending party to one or more receiving parties via an intermediate telecommunications system. Stated differently, e-mail is a means of sending messages between computers using a computer network. Electronic mail services, as defined in this policy, not only consist of the use of Municipality-provided e-mail systems but also the acts of sending and receiving electronic mail across the Internet.

Electronic mail is an efficient and timely communication tool that can be used to accomplish **WDM** functions and conduct the Municipality's business within its organization, with other governmental bodies, with private sector organizations, and with the public sector. E-mail can help the **WDM** improve the way it conducts business by providing a quick and cost-effective means to create, transmit, and respond to messages and documents electronically. Well-designed and properly managed e-mail systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. Daily tasks are accomplished more rapidly as individuals use e-mail services for sending and receiving texts as well as avoiding telephone expenses.

There are a number of characteristics that distinguish electronic mail from other means of communication, such as paper records, telephones and information stored on electronic media such as diskettes. Awareness of these characteristics should guide individual and Municipality use of electronic mail services.

2. Purpose of the Policy

The purpose of this is to establish guidelines, define users' roles and responsibilities as well as minimum requirements governing the acceptable use of the **WDM** electronic mail services. This policy specifically pertains to the use of World Wide Web on the Internet and the receipt, storage and distribution of electronic mail. By establishing and maintaining compliance with this policy, risks and costs to the Municipality can be reduced while the valuable potential of this communication tool is realized. The objectives of this policy are to assure that:

- The use of **WDM**-provided electronic mail services is related to, or for the benefit of the **WDM.**
- The use of internet and e-mal services contribute to the accomplishment of officials duties
- Users understand that e-mail messages and documents are subject to the same laws, regulations, policies, and other requirements as information communicated in other written forms and formats

- Disruptions to **WDM** activities from inappropriate use of Municipality-provided e-mail services are avoided
- Users are provided with guidelines describing their personal responsibilities regarding confidentiality, privacy, and acceptable use of Municipality-provided e-mail services as defined by this policy.
- Potential risk to sensitive system and or information is minimized to acceptable level.

3. Scope of the Policy

The scope of the policy covers those people who make use of WDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "USERS". Users are all permanent, contract and temporary personnel employed by the **WDM** who have been issued with a Municipality's Computer.

This policy refers to "Users" as all computer users at the WDM, whether they are permanent, on contract or temporary employees supplied by service-providers to the Municipality.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the Municipality's computers.

4. Background

The Internet resembles an alliance of public networks that employ a common set of protocols for the purpose of communicating information. The use of the Internet therefore offers a plethora of opportunities and benefits for Users to increase individual access to information resources relevant to official duties. However, the Internet is also subject to significant security problems as it provides potential access to a variety of information sources not relevant / related to official duties. Hence, not all resources on the Internet provide accurate, complete or updated information. Users are compelled to continuously evaluate the validity of information found on the Internet. It is therefore a general policy that Internet access and electronic mail services be conducted in a responsible, ethical and legitimate / lawful manner.

5. Policy Statement

5.1 WDM RESPONSIBILITIES

The **WDM** has the responsibility to ensure that Municipality-provided electronic mail services are used for internal and external communications, which serve legitimate government functions and purposes. The Municipality must familiarize each user with what is considered appropriate use of state-provided e-mail services. Managerial authority over electronic mail services must be defined, and user-training programs provided which address e-mail usage and policies. Municipality "E- mail Use Agreement" for electronic mail services, which stipulates compliance to this "Electronic

Mail Policy", must be signed by each user if they are to retain or be provided e-mail services. Failure to sign the use agreement will result in denial of electronic mail privileges for the individual. Any significant problems encountered in using e-mail communications should be brought to the attention of the ITO and where appropriate, **WDM** management should be notified.

5.2 USER RESPONSIBILITIES/ACCESS

5.2.1 This policy is intended to illustrate the range of acceptable and unacceptable uses of the Municipality's electronic mail facilities. Questions about specific uses related to security issues not covered in this policy statement and reports of specific unacceptable uses should be directed to the ITO. Other questions about appropriate use should be directed to the user's supervisor.

5.2.2 Users should be aware of potential electronic mail security problems before transmitting private or confidential messages. Electronic mail is not private communication. All information transmitted via the Municipality's Internet/e-mail system is the property of the Municipality and can be reviewed at any time. E-mail correspondence may best be regarded as a postcard rather than as a sealed letter. Disclosure may occur intentionally or inadvertently when an unauthorized user gains access to electronic messages. Likewise, disclosure may also occur when e-mail messages are forwarded to unauthorized users, directed to the wrong recipient, or printed in a common area where others can read them. Because of the various security, legal, and productivity issues referenced in this policy, each user has the following responsibilities:

- As an e-mail participant, each user must comply with this "Electronic Mail Acceptable Use Policy" and the Municipality's "E-mail Use Agreement" for e-mail services.
- Users must be aware of the classification of any information contained in data files or correspondence which they are transporting using e-mail communications and to not exchange information in un-encrypted form which is confidential.
- Under no circumstances should data ever be transported, which if intercepted, would place the Municipality in violation of any law.
- The content of anything exchanged (sent or received) via electronic mail communications (regardless of its state of encryption) must be appropriate and consistent with Municipality policy, subject to the same restrictions as any other correspondence.
- Users granted access to electronic mail services need to use that access in a way which is consistent with their job function even when the access is after-hours.
- E-mail communications, if allowed to accumulate on a server, can quickly consume the server's disk space and may cause system problems. Although deletion of unnecessary email communications is encouraged, users should consult the ITO regarding their record retention guidelines for proper instruction regarding disposal or archival of e-mail correspondence.
- Any Direct Connected Access to Internet and/or electronic mail services from official computers, networks and/or communication services must occur through accredited gateways or firewalls.

- No Remote (dial-in) Access is permissible due to security risks associated with dial in and out facilities.
- No remote or external connectivity will be allowed without prior knowledge of the ITO.

5.3 PRINCIPLES OF ACCEPTABLE USE

5.3.1 As with any Municipality-provided resource, the use of electronic mail services should be dedicated to legitimate Municipality business and is governed by rules of conduct similar to those applicable to the use of other information technology resources. Use of e-mail services is a privilege which imposes certain responsibilities and obligations on users and is subject to government policies and laws.

5.3.2 Acceptable use must be legal, ethical, reflect honesty, and show restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment and unwarranted annoyance.

5.3.3 All e-mail users should:

- Comply with Municipality policies, procedures, and standards;
- Protect others' privacy and confidentiality;
- Be responsible for the use of their e-mail accounts; and
- Use information technology resources efficiently and productively.
- Be courteous and follow accepted standards of etiquette. Users must abide by the etiquette rules but are not limited to the following:
  - Be polite
  - Use appropriate language
  - To refrain from revealing personal particulars about themselves or other Users to anyone else on the Internet
  - To refrain from revealing credit, credit checking accounts or identification numbers across the Internet
  - Not to attempt to gain illegal access to system programs or computer equipment
  - Use all appropriate precautionary measures to detect viruses and if necessary, prevent its spread.

6. USERS' ROLES AND RESPONSIBILITIES

By signing the "Acknowledgement Letter", the User acknowledges that he/she has read the terms and conditions of this policy and understands its significance. Access to Municipality Internet and electronic mail services is a privilege, not a right. The WDM Networks, Internet access and electronic mail services are to be used in a responsible, efficient and

legitimate / lawful manner and must be utilised to realise the objectives of the Local Government.

- Ensure that technical personnel from the ITO examine Internet traffic, electronic mail routing and information content in order to affect the legitimate performance of their official duties.
- Provide administrative assistance in the implementation of this policy.
- Understand and comply with the rules and conditions as set forth in the Policy.
- Not to add, delete or modify system files or change system setup on workstations made available to them.
- Not to log onto the Internet or use electronic mail using identification other than his or her own.
- Not allow any other person the use of his or her username and password to access the Internet and/or disseminate electronic mail from his or her official computer except when authorised to do so.
- To accept limitations or restrictions on computing resources such as storage space or amount of resources consumed.
- Not create access, display, download or transmit any text, image, or sound clip that include material which is obscene, libellous, or which advertises any product or service not permitted by law or that undermines the integrity and professional ethos of the municipality.
- Not to engage in any activities to damage hardware or software, disrupt communication services, waste system resources or overload networks with excessive data.
- Maintenance of Internet access and also the use of electronic mail services, content or otherwise, is constantly and vigilantly monitored and managed by the Information Technology Division to ensure quality and reliability of the systems. However, such monitoring may also be used to detect possible misuse thereof.

7. Privacy and Confidentiality

7.1 There can be no expectations of personal privacy or confidentiality in the use of Internet and electronic mail services since Internet access and electronic mail are subject to disclosure laws and record retention requirements.

7.2 All information generated by the User through the use of the municipality Internet access and electronic mail services will remain the property of the municipality.

7.3 Internet and e-mail access are monitored by ITO through a remote software to avoid people from abusing the services.

8. Acceptable Activities

8.1 Acceptable e-mail activities are those that conform to the purpose, goals, and mission of the **WDM** and to each user's job duties and responsibilities. The following list provides examples of acceptable uses:

- Communications, including information exchange, for professional development or to maintain job knowledge or skills;
- Communications with other Municipality's agencies providing document delivery or transferring working documents/drafts for comment
    - Announcements of Municipality procedures, hearings, policies, services, or activities;
    - Use involving research and information gathering in support of advisory, standards, analysis, and professional development activities related to the user's duties; and
    - Communications and information exchanges directly relating to the mission, charter, and work tasks of the Municipality including electronic mail in direct support of work-related functions or collaborative projects.
    - Limited personal use is allowed, subject to it conforming to this policy document.

NOTE:

- Users may be subject to limitations on their use of e-mail as determined by the appropriate supervising authority. Users are advised to remove themselves from electronic mailing lists not dealing with work- related topics.
- All electronic mail sent in the course and scope of the **WDM** business must be sent via the Registry Office.
- **No User is allowed to attach the Municipality letterhead with the Logo or Emblem**. No electronic signature containing the **WDM** details such as the letterhead should be attached to personal e-mail.

9. Unacceptable Activities

Unacceptable use can be defined generally as activities that do not conform to the purpose, goals, and mission of the **WDM** and to each user's job duties and responsibilities. Any e-mail usage in which acceptable use is questionable should be avoided. In other words, when in doubt seek policy clarification prior to pursuing the activity. The following list provides examples of unacceptable uses:

- Private or personal for-profit activities. This includes use of e-mail services for private purposes such as marketing or business transactions, private advertising of products or services, and any activity meant to foster personal gain;
- Unauthorized not-for-profit business activities. This includes the conducting of any non-governmental related fund raising or public relations activities such as solicitation for religious and political causes;
- Transmission of incendiary statements which might incite violence or describe or promote the use of weapons or devices associated with terrorist activities;

- Use for, or in support of, unlawful/prohibited activities as defined by Provincial and National laws or regulations.

Note: Unacceptable and forbidden User behavior regarding access to Internet and E-mail services encompass, but are not limited to:

- Using profane, obscene, pornographic or other graphic pictures, which may be offensive and / or defamatory to others
- Using the Internet to search, access, store and retrieve information that is racist, violent, offensive, sexually explicit (sexually explicit content includes e.g. Cartoons, Text Messages as well as Photographs)
- No User shall engage in/respond to- activities such as political/religious statements, cursing and foul language as well as statements viewed as harassing or discriminative based on race, colour, creed, age, sex, physical handicap and/or sexual orientation
- Copying commercial software in violation of copyright laws
- Allow his or her User account and / or User password to be used by another person unless authorised to do so
- Distribute material for commercial purposes
- Engage in any activity that could compromise the security of the Municipality's host computer
- Electronic mailing to groups of people for unofficial purposes (as such, sending large volumes of unsolicited e-mail is prohibited.)

Note: Illegal activities relating to e-mail and network access include, but are not limited to:

- The transmission of threatening, offensive or harassing information (messages or images) which contains defamatory, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
- Violation of laws dealing with copyrighted materials (including articles and software) or materials protected by a trade secret;
- Intentionally seeking information about; obtaining copies of; or modifying contents of files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;
- The transmission of any information which encourages the use of controlled substances or uses the system for the purpose of criminal intent;
- Violation of Provincial and National laws or regulations prohibiting sexual harassment.
- Violating the privacy of individual users by reading their e-mail communications unless specifically authorized to do so;
- Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by the ITO. Assisting others in violating these rules by sharing information or passwords is also unacceptable behavior;

- Deliberate interference or disruption of another user's work or system;
- The user must avoid any actions that cause interference to the network or cause interference with the work of others on the network. Users are prohibited from performing any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of system/network performance), or the introduction of computer worms or viruses by any means (use of programs with the potential of damaging or destroying programs and data);
    - Distribution of "junk" mail, such as chain letters, advertisements, or unauthorized solicitations; and
- Unauthorized distribution of Municipality data and information.

10. Security Implications

10.1 The use of electronic mail services exposes the **WDM** and users to network and, in particular, Internet related risks. Even with the extensive effort that has been made by the **WDM** to minimize known risks, there is no known way to protect the Municipality from all related risks. E-mail and network security is a joint responsibility of SITA, Outsourced ISP Service Provider, DPLG, DLGH, ITO and e-mail users. Transmission of electronic mail to locations outside of the Municipality's local area network may require the use of the Internet for transport. Since the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls. Confidential and sensitive information must not be included in e-mail communications unless proper, formalized security precautions have been established. It is the responsibility of the ITO to protect confidential and sensitive information where intentional, inappropriate, or accidental disclosure of the information might expose the Municipality or an individual to loss or harm.

10.2 Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of their e-mail account by unauthorized individuals. Passwords should be changed with regular frequency or in accordance with the **WDM**'s policy regarding the frequency of changing passwords. Obvious passwords should be avoided. When users are away from their desks, precautions should be taken to protect their accounts (preferably shutting down the PC).

10.3 Much on Security has been covered in the Information Security Policy.

11. Application of this policy

11.1 The ITO is responsible for the implementation and enforcement of this "Electronic Mail and Internet Policy". These duties include, but are not limited to:

- Investigation of alleged or suspected non-compliance with the provisions of this policy; and
- Suspension of service to users, with or without notice, when deemed necessary for the operation and/or integrity of the Municipality's communications infrastructure, connected networks, or data.

- The ITO is able and reserves the right to monitor and/or log all network activity without notice, including all e-mail and Internet communications. Therefore, users should have no reasonable expectation of privacy in the use of these resources. While the **WDM** will not regularly monitor electronic- mail, users are on notice that the maintenance and operations of electronic message systems may result in observation of random messages. E-mail messages are not personal and private. E-mail system administrators will not routinely monitor individual staff member's e-mail and will take reasonable precautions to protect the privacy of e-mail. However, management and technical staff may access a user's e-mail:
    - ✓ for a legitimate business purpose (e.g. the need to access information when a user is absent for an extended period of time);
    - ✓ to diagnose and resolve technical problems involving system hardware, software or communications; and/or to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.
    - ✓ by participating in the use of networks and systems provided by the **WDM**, users agree to be subject to and abide by policies governing their usage. **WDM** management will review alleged violations of this policy on a case-by-case basis.

11.2 Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the Memorandum of understanding on Conduct of Service 0f 1994.

11.3 Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

12. **Written Agreement Required**

Users having access to **WDM**-provided electronic mail services are advised that all such network activity is the property of the Municipality, and therefore, they should not consider any activity to be private. All users of e-mail services are required to acknowledge acceptance of and their intention to comply with this "Electronic Mail Acceptable Use Policy" by signing the Municipality's Information Technology User Declaration Agreement. Signed agreements will be kept on the user's personnel file and copies thereof must be forwarded to the ITO.

13. Commencement and Revision

This policy takes effect on "DATE" and will be reviewed annually. The policy may be amended from time to time. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on the company Intranet and/or by way of e-mail.

14. Annexures

14.1 ANNEXURE A - Mailing Lists

The following table identifies **WDM** Mailing Lists.

Mailing List
Executive Mayor
Speake**r**
Members of Mayoral Committee
Councilors
Municipal Manager
Manager/Head of Department
Assistant Managers
All other Officials

14.2 ANNEXURE B - Email Disclaimer

In future an email disclaimer will be appended to all outbound email. The disclaimer will read as follows:

> The information transmitted is only to be viewed or used by the person/s or entity to which it is addressed and may contain confidential and/or privileged material/information. The Sekhukhune District Municipality (**WDM**) reserves the copyright to all contents of the **WDM** information contained in e-mail messages. The views and opinions expressed in this transmission are those of the sender and do not necessarily represent the views and opinions of the **WDM**. The **WDM** cannot assure that the integrity of this communication has been maintained nor that it is free from errors, malicious code, interception or interference. Under no circumstances will the **WDM** or the sender of this e-mail be liable to any party for any direct, indirect, special or other consequential damages from any use of this e-mail.

GENERAL DISCLAIMER

1. The information provided on this web site is proprietary to Waterberg District Municipality and certain clients of and suppliers to Waterberg District Municipality.
2. The logos and trademarks included in this web site may not be used for any purpose without the express prior permission of Waterberg District Municipality or of the client or supplier to whom such logo or trademark belongs. Enquiries in this regard can be lodged with the Municipal Manager of Waterberg District Municipality, via this web site.
3. The information provided is provided without warranty of any sort, express or implied. By using this web site you confirm that you fully indemnify and hold Waterberg District Municipality and all of the other parties represented on this web site harmless from all and every claim arising from your use of this web site and the information provided thereon, including special, direct and indirect, and consequential damages. The web site and any web site linked to it are used entirely at your own risk. Links provided on the Waterberg District Municipality web site identifies resources and links to other web sites that would appear useful for our readers. The Waterberg District Municipality may provide links to other websites only as a convenience and the inclusion of any link does not imply the

Waterberg District Municipality's endorsement of such sites. Linked websites or pages are not subject to the control of the Waterberg District Municipality. The Waterberg District Municipality is not responsible or liable, directly or indirectly, in any way for the contents, use, or inability to use or access any linked websites or any links contained in a linked website.

4. You expressly undertake not to use this web site or any other web site linked to it or the information provided on it for any illegal purpose or to transmit or transfer any undesirable material or information of any nature or in any form.
5. Any software provided by means of this web site or any of the web sites linked to it is provided strictly subject to the license agreements and terms and conditions prescribed by the holder of the proprietary rights in such software, and you undertake to honour such rights and prescriptions of the proprietary rights holder concerned.
6. Waterberg District Municipality and the Waterberg Board of Directors do not necessarily share or agree with the views and opinions published on this web site or any linked web sites, as such views and opinions are published, in many instances, for information purposes only.
7. The Waterberg District Municipality web pages are frequently updated and improved. New content will be added as it is available. Although we will attempt to keep information in the Waterberg District Municipality web site accurate, the accuracy of the information provided cannot be guaranteed.
8. We welcome third party websites to link to the information that is hosted on these pages. It is expressly prohibited for any person, business, entity or website to frame any page on this website, including the home page, in any way whatsoever, without the prior written approval of the Waterberg District Municipality.
9. The Waterberg District Municipality reserves the right to change, modifies, add to or remove from portions or the whole of these terms and conditions of use from time to time. Changes to these terms and conditions of use will take effect upon such changes being posted to this website. It is the user's obligation to periodically check these terms and conditions of use at this website for changes or updates. The user's continued use of this website following the posting of changes or updates will be considered notice of the user's acceptance to abide by and be bound by these terms and conditions of use, including such changes or updates.

14.5 ANNEXURE E - Email Content Filtering

The following rules have been configured on the Orange box (Content Filtering Software)

- The following file extensions or attachments are blocked
  - Exe, pif, com, bat, cmd, reg, sys, ini, cpp
  - All movie and music types e.g. Mp3, wav avi, mov, mpg, ogm, Real Audio, windows media player streaming audio, flash
  - All files with pornographic material
  - Pornographic keywords
  - Attachments with pornographic url's

- E-mail exceeding 2Mb in size is blocked
- All spam email is blocked

14.6 ANNEXURE F: DECLARATION FORM

INTERNET & E-MAIL FORM
SEND THIS FORM TO THE IT MANAGER,

Please enter your personal details:

First Name	Surname	Employee No
ID No	User ID/Profile	E-Mail
Phone No	Fax No	Building
Department	Section	Town
Floor No	Office No	**Date Required**

☐ **APPLY E-MAIL INDIVIDUAL ACCOUNT**

☐ **APPLY INTERNET USAGE ACCOUNT**

DECLARATION

I understand and will abide by the Municipality **Internet and Electronic Mail Use Policy** and acknowledge and understand that any violation of this policy will be unprocedural, constitutes an act of misconduct and possibly an offence. I further understand that should I commit any violation, further disciplinary actions may be taken against me.

User signature: _____ Date: _____/_____/_____

Head of Section: _____ Date: _____/_____/_____

14.7. ANNEXURE G – ELECTRONIC MAIL USE AGGREEMENT

USER CONSENT AND ACCEPTANCE

1. I, the undersigned

1.1 acknowledge that I have received, read and understand the **WDM** Electronic Mail Acceptable Usage Policy and accept the principles set out in the policy as binding on me;

1.2 agree that the municipality may from time to time monitor, access and view all communications created, stored, accessed, viewed, received and/or sent by me using the WDM IT system and that I have no guarantee or expectation to privacy in using the department IT system in accordance with the terms and conditions of this policy;

1.3 understand and acknowledge that a violation of this policy may result in disciplinary action in accordance with the Municipality's disciplinary procedures, including possible dismissal, as well as civil and criminal liability.

Signed at on 2004

_____ _____

NAME **SIGNATURE**

_____

Witness

1. Policy Background

Information security is absolutely important for the Municipality's existence, its ability to deliver services and its ability to grow. Information used in the everyday business, information used in tactical positioning, information used in strategic planning and any other information must be protected. This information must also be secured and the integrity and the availability thereof must be assured at all times.

The aim of the IT security policy is to ensure that all security measures are implemented to protect the Municipality's data, information, knowledge, information technology infrastructure, software and information systems.

2. Outsourcing

2.1 BUSINESS AGREEMENT

When the responsibility for municipality's information processing is outsourced to any external institution or organisation, security controls and procedures shall be addressed in a business agreement between the parties to ensure that the security of the municipality and government information is not compromised. In contracting for ICT related services with external parties, the basic point of departure shall be that an institution shall select only those vendors who undertake to comply with the security measure set in this policy and any other applicable regulation or policy of Government.

2.2 BUSINESS REQUIREMENTS

The needs of the business process must be addressed by either a manual or computerized system. It is critical that the business requirements be clearly defined and documented, otherwise other issues may take its place, such as the recommendations of the IT partner or supplier, which has a valid, but separate agenda. In many cases, managers find it seemingly complex to document their needs beyond high-level requirements. However, by recalling the view of Information Security, the high level requirements may be refined further by specifying the needs of the system with respect to**,**

- **Identification and authentication**
- **Authorization**
- **Confidentiality** – who is able to see/amend what,
- **Integrity** – a system that is proven, tested and has security and fall back routines in case of need; and
- **Availability** – the system must be available (say) to users in multiple offices both on workstations and their laptops.
- **Non denial**

Access control should be established that would limit or detect access to critical resources (e.g. data, files, application programs, and computer-related facilities and hardware), which helps to prevent unauthorized modification, disclosure, loss or impairment of data.

Information Technology Division shall employ the prevention technique of isolating or segmenting the network with firewalls to block unauthorized incoming traffic, direct incoming traffic, and protect vulnerable systems. Information Technology Division will ensure that Anti-virus software are installed at the network perimeters and deployed to all workstations.

2.3 BASIC SECURITY REQUIREMENTS

Persons responsible for commissioning outsourced computer processing must ensure that the services used are from reputable companies that operate in accordance with quality standards which should include a suitable service level agreement that meets the requirements of WDM as regulated by government. The Contractual agreement shall include the following:

- The legal requirements to be met, for example data protection legislation.
- Arrangements to ensure that all parties involved in the outsourcing, including sub-contractors, are aware of their security responsibility.
- The measures for maintenance and testing of assets to ensure the integrity and confidentiality of institutional business assets.
- The physical and logical controls to be implemented to restrict and limit access to sensitive business information to unauthorised users.
- Measures to maintain the availability of services in the event of a disaster.
- The levels of physical security to be provided for outsourced equipment.
- The right of conducting a security audit.

3. Unauthorized Access Rights

A username is to be suspended immediately (or appropriate measure be taken to address the matter) when the individual user no longer needs access to the computer system or terminates employment with the municipality.

If users change work positions, their access rights will be reviewed and changed to match their new jobs. Management may restrict or extend computing privileges and access to their information resources. The Information Technology Division must be notified by head of department or the supervisor of the official concerned to suspend the user.

3.1 PROTECTION AGAINST UNAUTHORIZED ACCESS

It is the responsibility of Information Technology Division to ensure that WDM's systems and data are safe and secure from unauthorized access that might lead to alteration, damage, or destruction of automated resources and data, unintended release of data, and denial of service.

It is the responsibility of every user to ensure that the information and data in his/her computer are stored in a safe place and according to standards and circulars stipulated by Information Technology Division.

4. Movement Of Hardware

Any movement of hardware between the municipality's locations as well as off the premises is restricted and controlled by IT Office. A further critical consideration is the security of any information contained on it. Often, the data and information are more valuable than the equipment itself. Any person willing to move the equipment should do so with the permission of the IT Manager and his/her Head of Department. Movement due to relocation of offices shall also be reported to IT Office

5. Orientation

Information Technology Division should hold orientation sessions for the newly employed personnel before a password is given to the user. The training session will among other things include network login, e-mail and internet access, printing, file sharing etc. Additionally, one-on-one training or group training can be scheduled if there are drastic changes on the system especially those that need thorough communication to the user(s).

6. Email Security

Electronic Mail (Email) functions much like ordinary mail. The sender writes an electronic letter and may add, if needed, enclosures such as text documents, graphics or spreadsheets. The sender then 'posts' the message by adding the recipient's Email address, often selected from an electronic address book. These Email addresses may be people, departments or functions and include names and some indication of location.

Email uses resources that can be distributed over several data networks. The user's conduct contributes to whether or not the availability and confidentiality of the system is ensured.

6.1 RISKS OF EMAIL

Since e-mail includes both the transmission and handling of sometimes-sensitive information, care must be taken to protect the message from unauthorized access.

Threats can include the ability of individuals to change and copy information, or to distribute information to unauthorized parties. Users can also act anonymously, or with a fake identity, and spread information under assumed names.
The use of e-mail is therefore open to a number of commercial risks, including:

- Inadvertent change or distribution of messages through error or negligence
- Unauthorized use, processing or distribution of messages

- Distortion, interruption or unwanted disclosure of messages
- Unauthorized disclosure of confidential, proprietary or trade secret information

6.2 E-MAIL NAMING STANDARDS

The following naming standards have been agreed to and will apply for all WDM e-mail users:

- ✓ The surname and first initial of the user will be used as the e-mail id
- ✓ When defining a new username or e-mail id, if such name already exists, the second initial will be utilized.
- ✓ No nicknames will be used as network or e-mail id's.

Size Limits of Mailboxes, and Attachments

The following limits will apply and adhered to by all WDM e-mail users:

- A size limit of 10 MB for mailboxes.
- A size limit of 2MB for Sending and receiving mail, inclusive of original message plus attachments.

6.3 E-MAIL POLICY STATEMENTS

- Private use is permitted but this is subject to strict control. Abuse of this privilege may be regarded as misconduct.

- From time to time the use of the Email system may be audited.

- The Municipality reserves the right to inspect the e-mail at any time without notice.

- Through using Email you will have been deemed to have read, understood and agreed to the policies relating to e-mail systems contained within these documents.

- Do not as matter of course forward confidential, trade secret or proprietary information to third parties. Delete any unnecessary e-mail you receive from the Email system after having been read. Save the important e-mail attachment in My documents for future reference

- Do not send all messages as confidential as this negates the purpose and adds unnecessary overheads to the e-mail systems.

- Check any e-mail enclosures for viruses, BEFORE opening, particularly if documents containing executable programs are sent. If users open a message and are prompted to "Enable or Disable macros" users should select "Disable" and scan for viruses. If any Viruses are found then notify the Information Technology Office.

- If users get an attachment via Email, which is unsolicited, or of unknown origin, detach it and scan the file using the installed anti virus software. Alternatively delete it.

- Avoid unnecessarily large distribution lists.

- Check your mailbox regularly for received mail.

- Ensure that the content of the message cannot be misinterpreted and that there is nothing unlawful about the transmission or content of the message.

- **Always click send and receive every time once opening your Outlook**

- From time to time, certain disclaimers may be required for messages requiring confidentiality, legal privilege etc. Request assistance from the Municipality's legal Officer.

- It is prohibited to forward or transmit: Offensive, defamatory, discriminatory or harassing material, Sexually explicit or other offensive images, Unlicensed copyright material, non- business related video and image files, confidential, proprietary or trade secret information outside without authorization, advertisements and chain letters.

- Do not send or forward Email notices concerning virus or harmful code warnings to other employees.

- Avoid sending messages with large attachments. Large attachments can be compressed (with a utility such as WinZip).

- Do not send a large number of Email messages to a single address as it may disable the destination mailbox.

- Do not "broadcast" Email messages unnecessarily.

- When using electronic mail to communicate with people on the Internet:
  - Do not automatically forward internal mail to an Internet site.
  - Do not use auto-reply functions to respond to your Internet mail.
  - When using the auto-reply functions such as Out of Office message option for normal municipality's internal mail, be sure to select the option that excludes sending the notices to Internet users.

- Users shall not use an electronic mail account assigned to another individual to either send or receive messages.

- Users should regularly move important information from electronic mail message files to word processing documents, databases, and other files, as Email messages may be

erased periodically, either accidentally or as part of normal archiving and file maintenance functions.

- If users receive unwanted and unsolicited email (also known as SPAM), they shall refrain from responding directly to the sender. Instead, they should contact Information Technology Division.

- Email is a vital communications tool for the municipality. Users should therefore access their Email INBOX as often as possible. Unopened Email older than one calendar month will be deleted from the server.

- It is the responsibility of individual users to manage their own Email once they have downloaded it. It is suggested that unwanted Emails are regularly deleted and important Emails are moved to appropriate folders. Important attachments should be saved in an appropriate folder within the "My Documents" folder and saved to a network server for backup. Contact the Information Division should further information regarding the management of Email be required

- Mail access is approved for the municipality's employees and councilors with valid employee numbers only.

- Every outgoing message should contain a disclaimer at the end e.g. "All views expressed herein are the views of the author and do not reflect the views of the Municipality's unless specifically stated otherwise". "The information is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material.

7. **Internet Security Policy**

The Municipality's information, computing assets, and corporate image on the Internet are critical to our success, and as a result, must be protected from loss, modification or destruction.

The Internet is used to connect with our customers, suppliers and other organizations.
It is important to remember the following points:

- The Internet is used by millions of people worldwide.
- Unprotected information sent across the Internet may well be read by any number of unknown people.

7.1 RISKS OF THE INTERNET

On the Web, one of the real dangers is a possible loss of company privacy or leakage of information about the municipality's activities. The following issues relate to users privacy when surfing the web:

When users visit a web site, the site they are visiting can identify where their Internet connection originates. For example, if users use the Web from work, activities can be identified as coming from the municipality**.** Web sites can log all of users activity including any personal data they provide. The web site owner can associate users with this data on future visits. Some web sites do not respect data privacy laws and may make the information collected from you available to other organizations.

7.2 VIRUS

Viruses are designed at best to cause some discomfort and at worst to cause the alteration and loss of data on a computer. Viruses pose a tremendous threat and can be introduced in a number of ways, particularly from files and programs downloaded from internet sources and via email attachments. It is therefore imperative that all computers in use have approved anti-virus software loaded and activated, and that this software is regularly updated. Contact the Information Technology Division if you are in any doubt about either a message or file content or for more information about anti virus software.

7.3 INTERNET SECURITY POLICY STATEMENTS

- Only those employees who have received department management approval may access the Internet via the municipality's facilities. Automatic access to the Internet is not a right, and access can be revoked if it is found that misuse of the facility is occurring.

- Whenever an employee posts a message to an Internet discussion group, an electronic bulletin board, or another public information system, this message shall be accompanied by words clearly indicating that the comments do not necessarily represent the position of the municipality.

- Unless expressly authorized by the Municipal Manager, when using Municipality information and/or systems, all employees are forbidden from participating in Internet discussion groups, chat rooms, or other public electronic forums except for work related purpose.

- Users shall not advertise, promote, present, or otherwise make statements about municipality products and services in Internet forums such as mailing lists, news groups, or chat sessions without the prior approval of the Municipal Manager.

- Although the Internet is an informal communication environment, the laws for copyrights, patents, trademarks etc. apply. Employees using Municipality internet or communication systems shall:
- Resend material only after obtaining permission from the source.

- Quote material from other sources only if these other sources are identified.

- Reveal internal municipality's information on the Internet only if the information has been officially approved for public release by the municipality's Communication section.

- When using the municipality's information systems, or when conducting municipality's business, employees shall not deliberately conceal or misrepresent their identity.
- Information Technology Division may prevent users from connecting with certain non-business web sites. The ability to connect with a specific web site does not in itself imply that employees are permitted to visit that site.

- No user or independent contractor to the municipality may use the available Internet, Intranet or E-mail services provided by municipality to access newsgroups, Internet web sites and FTP sites for unauthorized and/or unacceptable purposes such as, but not limited to:
- The viewing and/or downloading of pornographic or obscene material of any nature;

- All software and files down-loaded from internet sources via the Internet (or any other public network) shall be screened with approved virus detection software before being run or examined via another program such as a word processing package.

- All users wishing to establish a connection with the municipality's computers via the Internet shall authenticate themselves at a firewall before gaining access to the municipality's internal network. Contact the Information Technology Division for further information.

- Non-municipality's computers are prohibited from connection to the municipality's networks without specific written permission from the Municipal Manager.

- Dial out or connections to any non-municipality systems or networks while simultaneously connected to the internal network are prohibited.

- Do not run security-testing tools/programs against any Internet system or server.

- Dial up connections e.g. whilst traveling or from home based systems and laptop computers which are also utilized for municipal business must only be made via authorized dial up procedures which employ the use of firewalls and configured by Information Technology Division.

8. **Passwords Policy**

- A computer access password is the primary key to computer security. The importance of password maintenance and security cannot be over emphasized.

- All employees and uses of the municipality's computer facilities are solely responsible for the integrity and secrecy surrounding passwords allocated for their usage.

- The password uniquely identifies employees and users, and allows access to the municipality's information and computer services. For your own protection, and for the protection of the municipality's resources, you must keep your password secret and not share it with anyone else.

- Contact the Information Technology Division if any further password information is required, or if there is any uncertainty surrounding the usage, applicability, installation or issuing of passwords.

- Users create their own password on their computers and IT Office have the right to reset, over-write once the user has forgotten or request it to be changed.

8.1 PASSWORD POLICY STATEMENTS

- All user-chosen passwords for computers and networks shall be difficult to guess.

- Construct fixed passwords by combining a set of a minimum six alphanumeric characters

- Do not construct passwords, which are identical or substantially similar to passwords previously used

- Passwords shall not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them.

- All vendor-supplied default passwords shall be changed before any computer or communications system is used.

- All passwords shall be changed immediately if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.

- Regardless of the circumstances, passwords shall never be shared or revealed to anyone else by the authorized user.

- Users: Are responsible for all activity performed with their personal user-Ids, Shall not allow the user-IDs to be used by anyone else and shall not perform any activity with other users' Ids.

- Employee and user generated passwords should in general have the following characteristics:
    - Be at least 6 characters in length
    - Contain at least one alphabetic and one non-alphabetic character
    - Not contain the user id as part of the password.
    - Be changed at least every 3 months for systems that do not automatically force regular password changes.

Normal windows screen savers should be activated after 10 minutes of inactivity as a maximum, and should be password controlled.

Certain systems e.g. Payday have specific password requirements over and above those shown above. These systems will prompt the user for the correct information. If in any doubt, contact the Information Technology Division for further information.

Should users forget their password, they must contact the Information Technology Division for assistance.

9. **Data Backup**

Therefore IT has to put contingency plans in place to take care or to prevent the loss of data critical to the business.

- Backups are done daily to ensure the restoration of data due to unforeseen events.
- BackupExec Software is used on Windows 2000 to backup data
- Backup tapes are used to store the data.
- Backup tapes are clearly labeled e.g. Monday, Tuesday, Wednesdays , Thursday , Friday
- On the Linux Server, backups is used the backup the Financial System data, as stipulated in the Financial System user manual
- Fully backup strategy is done once a week e.g Fridays and on the other days differential backup strategy is applied (Backup of data that has change since the last backup.
- Data to be backup has to be identified
- A backup schedule has to be implemented (When data must be backup, automatically)
- Backup logs (Print out proving that data has been backup) must be printed and stored for auditing purposes

10. **Disciplinary Action**

Users will be subjected to disciplinary measures if they violate this policy, and disciplinary action will be applied in a progressive manner in line with the Disciplinary Code and Procedures of the municipality.

GUIDELINES ON THE USE OF IT AND OTHER COMPUTER EQUIPMENTS

1. PURPOSE

The purpose of this document is to regulate the use of all IT related equipments and resources so that the Municipality can:

- Control costs with a standardized set of hardware and software that can be well supported and maintained;
- Use IT equipments economically and productively;
- Minimize risk in terms of loss, stolen, damaged equipments.

2. WHO IS AFFECTED?

Every employee of the Municipality, Councilors, Temporary Staff, Consultants who are in use of any form of IT equipment will be affected by this document.

This document must also be applicable to all those IT service providers contracted to the municipality, whose personnel have access to our computers.

3. PROCEDURE AND GUIDELINES STATEMENT

3.1 ALLOCATION IT EQUIPMENTS

Through a request from your manager, you may be issued with a computer and other IT related equipments or resources. All are provided to you to help you perform your duties effectively and efficiently so.

Allocations of computers to officials will be according to the Municipality's IT equipments standards document or guidelines as addressed in the IT Asset Management Policy, however if you need a non-standardized equipments, then a recommendation should be made to the ITO. All equipments provided to users by ITO will remain the property of the Municipality and can be re-allocated to perform another task if need arises.

No procurement of computer-related equipment and software shall take place without an appropriate recommendation from the ITO.

3.1.1 LAPTOP ALLOCATION

The use of personal computers and laptops has become an integral part of fulfilling an employee's daily task and responsibilities. To this end, the municipality provides employees with the access to personal computers or workstations to enable them to fulfill such duties and responsibilities.

In certain instances, the nature of an employee's job necessitates access to a notebook (portable personal computer) or handheld computer. This document serves to clarify the municipality's approach regarding WDM provided notebooks. Management reserves the right to amend or provide exceptions to this document in specific instances.

3.1.1 Allocation of note pad.

-
- Employees who require access to portable personal computers for the purpose of fulfilling their normal daily responsibilities
- In this case a motivation has to be submitted to the Information Technology Division through the Head of Department.
- Laptops remain the property of the municipality and must be returned on the employee leaving the employment of the municipality. The staff member is responsible for ensuring all appropriate steps are taken to avoid accidental damage or loss to the laptop. All other employees who are required to use or have access to computers will only be given access to desktop personal computers or computer workstations.

3.1.2 PRINTERS

Printers will be allocated to officials depending on their specific needs. Colour Deskjet printers will be allocated to those who frequently needs to print colour documents, other officials will be required to use the Central Colour Laser Printer.

3.2 STANDARD OF EQUIPMENTS

Acquisition of software and hardware must adhere to the municipality's standard to avoid user's personal preferences and determine the choice of hardware and software.

The standards document specification will be revised time to time, as and when the need arises.
The standards document will cover the following areas

- Specifications of the required desktop computer, including printers, notebooks, and other IT related equipments.
- The manufacturer or brand of the equipment.
- All standard software, systems, databases used in the district.
- Critical and non-standard software and other IT equipments.

If the Information Technology Division approves to raise the standard, all computers below the standard will be upgraded or replaced, without the need to motivate.

The goal is to obtain the best value for the product, better-negotiated service agreement and adequate support. It may also be required to purchase particular products from selected vendors/manufacturers because of the support and services offered (For example, only IBM Desktop computer will be purchased due to warranty provided by IBM). Though these will be centrally managed, all purchases should adhere to other numerous WDM policies, procedures and/or any other applicable regulations or acts of municipal government.

Analysis of hardware may include: -

- Appropriate software for the required task.
- System that comply with Technical Architecture or IT Strategy (Information security issues).
- Value for price, performance, reliability, adequate capacity and support issues due to unexpected failure of hardware.

Long term organizational business needs must be taken into account since it is expensive to make subsequent changes.

3.3 NEW POSITION AND APPOINTMENT

When appointing a new employee for whom a computer is needed, and during resignation, Human Resources must immediately notify Information Technology Division after the decision has been taken to fill or create the post. Such notice must be in writing accompanied by detailed job description of the incumbent. When replacement positions are filled, the new appointee will be allocated with the computer that went with the position. If any changes/upgrades are required to meet the needs of the new employee, it will be responsibility of Information Technology Division to fund hardware and/or software to meet these needs before the incumbent resumes his/her duty.

3.4 COMPUTER AND SOFTWARE MAINTENANCE

Information Technology Division will maintain records of all hardware warranty and software upgrades agreements. Any computer system and its peripherals purchased through Information Technology Division are covered and should be serviced by the vendor during the warranty period. The cost of ordinary repairs beyond the warranty period should be paid from ITO budget. Severely damaged equipment will require special evaluation (e.g. if the damage is such that it goes beyond the value of the equipment, it is better to replace the equipment than repairing it). Information Technology Division will only perform software or hardware upgrades or maintenance on any equipment that has a Municipality's asset register sticker attached. No installation or maintenance of hardware or software can be performed on privately owned personal computers

The Municipality retains the exclusive right to determine the hardware and software configuration of any personal computers purchased or funded by it, including any peripherals hardware such as modems, network accessories, printers, etc and may in its sole discretion determine the price range and approved suppliers of laptops funded or purchased by or through the institution. No software may be installed on any computers owned by the municipality without first ensuring that the municipality has the necessary software licenses of such software. The installation of any additional software must be weighed against the anticipated benefit.

However, management reserves the right to amend or provide exceptions to this document in specific instances.

3.5 MAJOR PROJECTS

Cost related to infrastructure changes, renovations, or office moves (e.g. re-cabling or installation of additional network points) must be included in the projects and will not be paid from the ITO Budget. Major cabling projects should be budgeted for and handled in conjunction with municipality's procurement policy for large spending e.g. cabling of the new premises.

3.6 PERSONAL USE IS ALLOWED SUBJECT TO THE FOLLOWING CONDITIONS

- Personal use should not affect service delivery.
- Personal use should not cause the municipality to incur direct cost.
- Personal use must again comply with the content of this document.

3.7 USER'S RESPONSIBILITY

Users will be expected to take care of the equipment issued to them. This is particularly more relevant to staff who use portable equipment such as Notebooks.
If the user loose or damage equipment or software that belongs to the Municipality it must be reported to Head of Department, the head will then inform the Information Technology Division. *In case of theft or suspected theft, users must also report it to South African Police Services.*

Users may have to pay for lost, damaged or stolen Notebook or equipment if

- They have acted negligently.
- Intentionally caused the damage.
- Ignored any pre instruction given (This include Municipality circulars).

In case the user requires Municipality's computer outside the premises, either to work at home or at another site/building, the user must obtain written permit or authorization from the Head of Department and Approval from IT Manager, before the equipment is removed. The permit must indicate your name as well as the description of the equipment to be removed, the date of removal and of return date.

3.9 INAPPROPRIATE MATERIAL

Users are not allowed to store information or material that can be considered offensive; this includes words, images or recorded sounds.

Users must avoid storing files that has any form of the following information, Political opinions, pornography, violence, nudity etc, it might cause bad working environment.

The above might have been stored on your computer by another user, either accidentally or in violation of the document, and you accidentally view the material, the Municipality won't

be responsible for that. ***If you discover this kind of offensive things in your computer, you must report it to ITO.***

3.10 MANAGERS'S RESPONSIBILITY

- Managers have the right to monitor the use of computer equipments and software by officials within their departments.
- Managers must ensure that all their computer-using staff, temporary or permanent is made aware of this policy. The Managers are required to apply the policy to all those who report to them.

3.11 GRANT FUNDING

A department preparing a proposal for funding involving computer hardware and/or software should consult Information Technology Division. IT Division will assist in identifying hardware/software that is supported and will work best on the infrastructure.

3.12 DO N'T S AND DO'S

You are not allowed to

- Bring your home computer along to the office.
- Move your computer without informing the ITO.
- Put your coffee/tea cup on top or close to your computer.
- Disconnect your PC for a reason not known to the ITO.
- Install a third party software or non-standard software, unless authorized to do so.
- Install computer games or other entertainment software.
- Repair or perform any form of upgrade to the computer equipment.
- Swap computer equipment with other officials.

You must

- Switch off your computer when you knock off.
- Be logged into the network when using a computer.
- Obtain a permit before taking an equipment offsite, unless it is a notebook officially allocated to you.
- Always keep your desktop computer tidy.
- Inform Information Technology Division if you suspect something wrong with your equipment before it is too late.
- Report any unlicensed or suspected non-standardized software to the Information Technology Division.
- Clean your computer Keyboard, Mouse, System Unit and Monitor using the approved equipment as supplied by ITO.

3.13 APPLICATION OF THE PROCEDURES

The procedures will be applied in different ways including:

- Where technology allows, this will be enforced automatically e.g. people will be prevented from running executable files, automatic lock of critical areas of your desktop etc.
- Information Technology Division monthly reports will highlight possible violations. The offender's manager will take disciplinary action in line with Municipality's disciplinary codes.
- Users will be expected to report any violation.
- The Information Technology Division may issue instructions via Corporate Services Manager.

3.1.4 DISCIPLINARY ACTION

Users may be subjected to disciplinary measures if they violate these guidelines, and it will be in line with the Municipality's disciplinary codes.

PROCEDURE MANUALS

Problem Management

- Logging IT / IT Related Calls
- Please note that all end-users are expected to try and diagnose IT problems encountered before calling the IT Office.
  The following shall be checkpoint for users before a call is logged
  (in the order they appear): -
- All cable Connections
- All peripheral connections
- Power connections
- Reboot if possible (Switch off the plug on the wall socket)

WDM Call logging procedures

Users call log on procedures

- User determines problem.
- Phone the IT Office.
- Explain the problem.
- IT Office offer first line support. (If problem solved is closed, if not escalated to Technician)
- Receive the reference number and name of technician.
- Technician liaise with the user, solve the problem, if not liaise with other team members, if not log with service providers.
- IT Office makes a follow up call (if necessary).
- Close the call (IT Office).

The turnaround time for IT service delivery is specified in 5-20 minutes depending on the location. The IT staff and the IT Office shall be measured as such.

3. *End-User Procedures*

A. Network & PC Storage

Note that all business files shall be saved in the network folders –"Home directories or other designated folders".

1. Saving Files (First time only)
The WDM Information Technology system has been standardized to
Microsoft XP Professional and Microsoft Office XP Professional across the organization.

All Microsoft Windows applications (used in the WDM) follow a similar
procedure for saving files.

In the application e.g. MS Word, Excel, Power point, Access and Projects: -

- Click the **"File"** in the menu bar or click the **"save"** icon in the standard bar.
- Click save (a "save as" message box will appear),
- Make sure of the location either my documents or your Stiffy Drive
- (A drive) and name the file appropriately,
- Click the "save" button.

2. Resaving files

- Click "file ","Save"
- Click the "Save" button in the standard menu bar or

3. Resaving Files (As a different name)

- Click "File",
- Click "Save As"
- Click the "Save AS " message box, change the file name
- Click the "Save Button"

4. Open Saved File

- Click File,
- Click Open,
- Select the Saved File, and
- Double Click the File.

5. Print

- Click File
- Click Print

5. Deleting Files

Deleting network files is permanent. Take care to ensure that you really want to delete these files. Deleting of PC files places them in the recycle bin.

- Double-click the "My Computer" button
- Navigate to the folder where the file to be deleted is located,
- Click the file once only (it will be highlighted / selected),
- Press the "Delete " button in the keyboard,

Confirm deletion by clicking the "Yes" in the confirmation window.

NB: A number of files can be selected at the same time by keeping the "Ctrl" button. Depressed and selecting various file one by one.

NB: Business files are to be saved in the network for security and backup purpose.

B. Handling E-mails

1. Creating new Mail

Inside the e-mail application "outlook"

- Click the "New" icon-a blank window for new mail will appear,
- Enter the correct destination e-mail address,
- Enter the correct Heading / Subject for your correspondence,
- Attach a file in necessary (see point to below on how)
- Click the "send" button.

2. Deleting Mail

Deleting mail is the same as deleting file in windows

- Inside the e-mail application "Outlook
- Click the folder on the right hand column
- Right click the mail item to be deleted
- Select Delete or
- Alternatively –select the mail item and press the delete button

3. Attaching Files

Attaching files that you bring an external, ready-made file into your e-mail message. There are three ways to do this: -

Inside Outlook

- Make sure that the cursor is at the right location
- Click the Attach in the – a message box insert file will appear
- Navigate to correct location and click file to be attached
- Click the Insert button

This will take you back to Outlook with the file attached
Continue as usual

Inside a Windows application
Without having opened outlook, the action defined below will open a new e-mail message with the attachments(s) already inserted
Inside for example Ms Word – with the document already typed

- Click file
- Clicks send to
- Click Mail Recipient (As Attachment)

A new e- mail message with the attachments will open up
Just fill in the other fields as usual and proceed

From any folder e.g. desktop C:\, H:

- Navigate to the folder that contains the file (s) to be attached,
- Right click the files and select send to
- Click mail recipient

A new e-mail message with the attachments will be open
Just fill in the other fields as usual and proceed
4. Opening Attachment Files
Attachments will generally be at the bottom box of E-Mail window. It happens however that an attachment will be located inside the message box.
Double click the attached file to pen it
Outlook will sometimes ask you if you want to open or save the file
Select the appropriate option and follow the usual process

NB: Windows will automatically detect the type of the file and open it using the right application.

5. Creating E-mail Folders
Creating folders in Outlook is similar to creating folder in the "Windows Explorer". Please note that there are sub-folders with folders. The main folder contains a "+" sign indicating that there are sub-folders in that folder. The "-" sign indicates that the subfolders have been.

- Right click the folder in which you want to create a folder,
- Click at "New Folder",
- Enter the appropriate name for the folder to be created,
- Click the "OK" button,
- The folder will appear back in outlook.

6. Moving Mail
Folders can be created to organize mail storage. Archive folders are created to facilitate organization of mail files. These folders are created outside outlook – in the home directory folders (to lesson storage burden in the mail serve).
Once the archive folder is in place, the following procedure is followed: -

- Note the folder marked 'Personal Folders' and all its contents,
- Select the mail files(s) to be moved from the right hand column,

- Press and hold the left button of the mouse and drag the selected items
- to the desired folder (into the right hand column) in the folder marked
- Personal "Folders" Selected items will be moved

1. Deleting Mail

Make sure that a correct folder is selected e.g. Deleted Items or Inbox
Select the file to be deleted on the right hand column and press delete key'
If the deletion is made from any folder than the Deleted Items", files will be deleted without any message box popping for confirmations. Files are placed in the "",
If the deletion is made from Deleted Items, a message box will pop up require ring confirmation that the files are in order to be deleted. This deletion is permanent. Files will be removed from the folder.

6. Archiving

This action will frequently be conducted by all staff purposes of saving their mail for longer periods. This action lessens the workload on the Mail Server in that all archive storage's take place at the File Server instead of the Mail Server.

Signatures

ENDORSEMENT

Policy **ENDORSED** by the Corporate Portfolio Committee on the ……..
…… …….
Chairperson: Corporate Portfolio Committee Date

APPROVAL

Policy **APPROVED** by the Mayoral Committee on the ……..

……. …….
Executive Mayor Date

ADOPTION

Policy **ADOPTED** by Council Meeting on the ……..

.....	.....
Executive Mayor	Date