ICT ACCEPTABLE USE POLICY

APPROVED BY:

MR M NAKO

MUNICIPAL MANAGER

DATE: 21/06/2023

APPROVED BY:

CLLR S JANDA

EXECUTIVE MAYOR

DATE: 21/06/2023

1. POLICY BACKGROUND

Effective and proper use of information technology is fundamental to the successful and efficient running of the Municipality. However, misuse of information technology – in particular misuse of e-mail and access to the Internet – exposes the Municipality to liability and is a drain on taxpayer's resources. It is critical that all users read and understand this policy and make themselves aware of the requirements and regulations.

Across a wide spectrum of industries and countries, Information Communication Technology (ICT) is transcending its traditional "back office" role and evolving into a "strategic" role with the potential not only to support business strategies, but also to shape new business strategies including service delivery in government and other service industries.

The government of the Republic of South Africa recognises the important role of ICT and has specified electronic government regulations in Chapter 5 of the Public Service Regulations of 2001, as amended on 15 December 2006. The key principle in the regulations states that departments should manage information technology effectively and efficiently in such a way that it leverages service delivery.

2. POLICY PURPOSE

The purpose of the policy is therefore to inform staff about their roles and responsibilities in using ICT tools/facilities provided to them by the Municipality.
To inform all computer users (employees, contractors, secondments, visitors, etc) about policies relating to the provision, use, replacement, and disposal of computer equipment and facilities.
The Municipality commands to ensure that the ICT resources provided to staff are utilised to enhance service delivery, increase productivity and improve the cost effectiveness of processes in the municipality.

3. DEFINITIONS

ICT	Information and Communication Technology
WAN	Wide Area Network
LAN	local area networks
EA	Enterprise Agreement
PC	Personal Computer
CPU	Central Processing Unit
VPN	Virtual Private Network

4. APPLICATION AND SCOPE

Mbhashe Local Municipality through the Municipality's Information Communication Technology office maintains computer networks and connections to the Internet through which users get ICT services. The Municipality's computer network consists of a backbone Wide Area Network (WAN), local area networks (LANs), as well as personal desktop and portable computers.

Municipality's ICT office has the sole responsibility of managing ICT resources and therefore provides access to computer networks and maintains equipment. In fulfilling its role, Municipality's ICT office aims to ensure that rights and responsibilities connected to computer usage are not violated.

Access to the Municipality's computer systems imposes certain risks and vulnerabilities. It follows that use of ICT services should always be legal and ethical; and reflect professionalism, honesty and integrity. Usage should also preserve respect or intellectual property; ownership of data; system security mechanism; and individuals' rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance.

It is the responsibility of all users of the Municipality computing facilities to be aware of and follow all ICT policies and guidelines, and seek advice in case of doubt. The ICT policies are published on the Municipal website, i.e http://www.mbhashemun.gov.za

This policy will be regularly updated or supplemented by specific standards or procedures to reflect further developments in technology or legislations that constitute this policy seek to provide for the mutual protection of the Municipality and the rights of its employees.

5. LEGISLATIVE FRAMEWORK

- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Data Protection Act 1998
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights Act 1998
- State Information Technology Act (Act no 88 of 1998)

- SACSA/0901/1(4) "Communication Security in the RSA"
- Protection of Information Act (Act no 84 of 1982)
- Protected Disclosure Act (Act no 2 of 2000)
- Copyright Act (Act no 98 of 1978)
- National Strategic Intelligence Act (Act no 39 of 1994)
- National Archives and Records Service Act (Act no 43 of 1996) as amended
- Provincial Archives and Records Service Act, (Act no 7 of 2003)
- Minimum Information Security Standards (MISS)
- Public Access of Information Act
- Promotion of Administrative Justice Act
- State Procurement Policy
- Electronic Communications Translations Act
- Comsec Act

6. POLICY PROCEDURE

This policy is applicable to ICT infrastructure and employees, including service providers offered systems to the municipality

7. GENERAL POLICY PROVISIONS

7.1 Ownership

Computing facilities owned by the Municipality and software including data developed (for whatever reason) on that equipment remains, in all respects, the property of the Municipality. The Patents Act 1978 and the Copyright Act 1978, Intellectual Property Laws Rationalisation Act 1996 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

Each user will be required to sign, as an indication to the Municipality, that they have read and understood the policy relating to ICT resources on a form.

8. PROCEDURES FOR IMPLEMENTING POLICY

8.1 ICT Procurement Policy Statement

The Municipality's objective is to carry out procurement of ICT goods and services in a way that:

- Delivery value for money
- ICT investment
- Maintains the highest standards of integrity
- Is competitively neutral
- Manages risk; and
- Is consistent with government requirements.

As one of the largest purchases of the ICT goods and services, the Municipality recognises the need for its procurement practices to encourage greater innovation, reduce costs to business and redress any unfair advantage to particular sections of the market.

8.2 Issuing of Computer Equipment

The issuing of computers to personnel in the department is based on the work requirement as well as the position of the official. All employees at management level are automatically issued with laptops once they either join the Municipality or are promoted to that level. Employees at positions lower than the management are issued with either a laptop or a desktop depending on the requirements of their work. A request for either a laptop or desktop must be approved by the Senior Manager Corporate Services and sufficiently motivated by the section manager and recommended by Senior Manager of the department. As such, it is the duty of the Senior Manager of the department to ensure that motivations and approvals are valid and that government-computing resources are allocated in a way that enhances effectiveness and efficiency.

8.3 Replacement and Disposal of Computer Equipment

Keeping up with the advances in computer technology is a never-ending challenge and no matter how much money Municipality spends on computer equipment; the equipment will eventually become obsolete. There is a computer replacement programme to ensure that the computer resources of the Municipality are always relevant, up-to-date, and effective. The policy is evaluated whenever necessary to ensure that appropriate facilities are available to staff in the municipality. The evaluation is done by collecting information through feedback from users, external vendor and industry resources, and departmental priorities. Before any computer is replaced there should be a supporting assessment report from the IT section.

8.3.1 Goals of computer replacement

The overall goal of computer replacement is to ensure that the computing resources in the municipality are up-to-date and available to relevant staff. The specifics of computer replacement are as follows:

- To ensure that each staff member is issued a computer of sufficient capability to support basic computing needs in fulfilment of work responsibilities;
- To implement minimum standards for computing resources and hence increasing the supportability and maintainability of the municipality's base equipment;
- To streamline specification, acquisition, and deployment of new equipment and re-deployment or disposal of old equipment.

8.3.2 Computer Replacement Guidelines

- **Computer Specifications**

The specifications for standard computing resources are developed each year by ICT section of the Municipality. Municipality officials are provided computers of standard specification and configuration.

- **Exception to Standard Equipment**

There are cases where standard equipment does not meet a specific requirement, such as a requirement for a specific platform because of disability or some other reason. Exceptions to the standard specification must be sufficiently motivated by the user and the supervisor; and are granted depending on the merit by the Senior Manager Corporate Services.

- **The Replacement Cycle**

The ICT section seeks to provide adequate technology for employees. It is generally expected that equipment will be replaced once every three years. The volatility of the computer industry and scarcity of resources may require lengthening this life cycle, as such; it is difficult to say definitively that a three-year cycle will be observed.

- **Replacement Notification**

Once computers that are due for replacement have been identified, a circular will be sent informing managers of the respective departments and providing a list of the currently available standard configurations for the new equipment. Departmental heads are encouraged to discuss the standard configurations with their staff and propose configurations that will most effectively meet their work requirements to ICT section.

- **Platform Selection**

The standard configuration is Microsoft Windows 10 or any latest Microsoft Windows operating system available. The ICT section has an Enterprise Agreement (EA) with Microsoft under which the latest versions of Microsoft are available to the Municipality. This means that the Municipality has up-to-date versions of Microsoft Office Suite, and other related software at any time.

- **Equipment Selection**

The standard configurations include both desktop and laptop models. While desktop computers have higher performance, laptop models are highly portable. The ICT section provides full support for both types of computers.

The following guidelines should be used to clarify the use of each configuration:

- The standard desktop is intended for general office productivity, such as word processing, spreadsheets, electronic messaging, and web browsing, making it suitable for most office needs.
- The laptop configuration combines basic office productivity with portability. The standard laptop configuration is suitable for staff whose jobs require them to use the computer in the office as well outside the office.

- **Resource Procurement**

Computers are purchased by the ICT section using capital budget. Newly acquired computers are delivered to ICT section where they are installed with standard software and configured for use on the network

- **Redeployment and Disposal**

Computers that have been replaced will be disposed according to Supply Chain management Policy or Asset Management Policy.

8.4 Software Piracy

The Municipality neither condones nor tolerates the unauthorised copying of licensed computer Software by employees. The unauthorised use of software is a violation of copyright Law, and May expose the individual and the Municipality to legal processes. The Municipality must adhere to its contractual obligations and comply with all copyright laws.

An employee who violates this policy may be subject to internal disciplinary action and could possibly face additional civil or criminal liability. For more information about whether particular activities are permissible or violate this policy, please contact the ICT Office at Ext. 5825 / 5872 before proceeding.

8.5 Services and support

All user support calls must be logged on helpdesk@mbhashemun.gov.za or EXT no. 5825 / 5872 during working hours. After work and weekends you can still get support by contacting ICT officials for urgent cases:

Manager ICT – 0647560614
System Administrator – 0824369981
IT Technician – 0825648939

8.5.1 Desktop PC's

Desktop PCs are critical assets to the Municipality. As such they must be managed carefully to maintain security, data integrity, and efficiency. All computers are supplied with relevant software installed on them. Users must consult ICT Office before installing non-standard software on computers. Non-standard software shall be interpreted as any software that is not included as part of the software for the computer when it is issued.

All users' files are automatically stored on the Municipality's backup server. Every time a user logs on to the network, files on the user's PC are synchronised with those on the server to make sure that the files on the server are always up-to-date. Users who generate much data are encouraged to request external hard drives to regularly back up their data in addition to the server backups.

Desktop PCs include the CPU/hard-drive unit and monitor both of which are barcoded components and are further subject to change control. Users must contact ICT Office before they can perform a transfer or swap of these assets.

8.5.2 Laptops and Notebooks

Portable PCs are at high risk from loss or theft and such require additional security protection. All reasonable precaution must be taken to ensure that hardware is stored securely. Each portable PC is supplied with security chain (lock cable) with which it must be secured at all times. Furthermore, the office must be locked every time the user leaves the office, even if it is for a few minutes, to ensure that nobody just walks in and takes the laptop or notebook.

Highly confidential data must be encrypted to protect the data in the event of loss of the portable PC; ICT Office is ready to assist with this process. If a user's portable PC is lost, ICT Office must be notified in writing with a copy of the police statement attached to the notification. In case a user's laptop is stolen from the office and there is no evidence of forced entry or breakage, the user will be charged with negligence in line with the Municipal Finance Management Act (MFMA). Once the case has been reported to ICT Office, it is then forwarded to the Asset section of the Municipality for assessment and further claim from municipal insurance. If it has been determined that a user was negligent in handling the PC, the user concerned should incur the replacement or fixing costs.

Users are responsible to ensure that laptops and any other computer equipment are secure outside the office. Laptops with broken screen or liquid affected all users will incur the costs to repair the device.
Laptop bags and other accessories should last at least up to three years.

8.6 Software

Only software properly purchased and approved by ICT Office may be used on the Municipality's hardware. Non-standard or unauthorised software can interfere with the stability of the Municipality's computing systems and network. Users who need extra software should contact ICT Office for assistance.

The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licenses must always be adhered to. Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without full comprehension of the user. Users discovering software that has been installed in an unsolicited manner are encouraged to inform ICT Office.

Standard Approved software's to be installed are:

- Microsoft Office suite (2016 upwards) 32bit and 64bit
- Desktop and Laptop backup application software (Cibecs)
- PDF (Adobe Acrobat Reader)
- Windows 10 Pro (32bit and 64bit)
- Financial Management System (SAGE 200 Evolution)
- Payroll and HR System (SAGE 300 people)

- Antivirus (ESET Endpoint Antivirus)
- Remote Support solution (TeamViewer and AnyDesk)
- Video Communication software (MS Teams and Zoom)
- Email Solution (Mimecast for Outlook)
- And any other approved software or application by ICT to support service delivery.

8.7 Data Security

Users must only access information for which they have been properly authorised to do so to perform their duties on the Municipality's systems. Under no circumstances should a user disclose personal or other confidential information accessible to them to unauthorised persons. The unauthorised access to and/or modification of data are a criminal offense under the Computers' Misuse Act 1990. It is the Municipality's policy to store data on a network drive where it is regularly backed up and secure. When an employee leaves the municipality is not allowed to delete any municipal information from either desktop or laptop.

- **Personal data and data protection plan act**

Data protection is an aspect of safeguarding a person's right to privacy, which is enshrined in the constitutional Bill of Rights. The essence of data protection is to give a person a degree of control over his or her personal information. However, the law also considers such competing interest as administering national social programmes, maintaining law and order, and protecting the rights, freedom and interest of others.

The Act stipulates that personal data shall:

- Obtained and processed fairly and lawfully
- Held for specified law purpose(s)
- Not used or disclosed in a way incompatible with the purpose(s)
- Adequate, relevant and not excessive for the purpose(s)
- Accurate and up to date
- Not kept longer than necessary
- Available to the date subject
- Kept secure

Staff should note that all data and correspondence, including e-mail messages, held by the municipality might be provided to a data subject, internal or external, in the event of a request for purposes of legal proceedings or other government-mandated requirements.

8.8 Virus Protection

Anti-virus software is installed on all computers as standard and is updated regularly via the network and internet. Anti-virus software must not be uninstalled or deactivated. Files received or sent by e-mail are checked for viruses automatically. Remote users are

responsible for maintaining up to date virus definitions on their computers and can contact ICT office for help as required.

Users must not intentionally access or transmit computer viruses or similar malicious software. Non-municipal software or data files intended to be run on the Municipal equipment by external people such as engineers or trainers must be checked for viruses before use. Where a user suspects a virus infection on a computer, ICT office should be contacted immediately.

8.9 Network

Passwords protect Mbhashe Local Municipality systems from access by unauthorised people: they protect user's work and the municipality's information. Therefore, users are to refrain from giving network password to anyone else.

Procedures are in place to ensure that users change passwords on a regular basis, passwords are of a minimum length and old passwords cannot be reused. Mbhashe Local Municipality does not allow the connection of non-corporate computer equipment to the network without prior written request and approval by ICT Manager. This includes connection via Virtual Private Network (VPN).

Further general guidance

Mbhashe Local Municipality users must ensure prior approval by IT Office to:

- set-up website on Mbhashe Local Municipality computing facilities
- publish pages on external world wide web sites containing information relating to Mbhashe Local Municipality
- enter into agreements on behalf of themselves or Mbhashe Local Municipality via a network or electronic systems
- transmit unsolicited commercial or advertising material to other users of a network or to other organizations
- installation of application/systems by service suppliers.

8.10 Internet Usage

The laws regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services, and tax apply equally to on-line activities. Strictly, documents must not be published on the web which are defamatory or which may constitute intimidating, hostile, or offensive material based on sex, race, colour, religion, national origin, sexual orientation, or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Strictly; material must not be accessed from the web, which would be objectionable on the above grounds under the self-governing law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks. Given the impracticality of accessing the exact legal position with regard to the previous two paragraphs, Mbhashe Local Municipality Acceptable Use Policy governing

material that could be objectionable on the above grounds is grounded in Constitution of the Republic of South Africa, Act 108 of 1996. On the basis of the constitution, then it is reasonable to expect Mbhashe Local Municipality employees to have good awareness and to be able to exercise good judgement. If in doubt over a specific case please enquire more information from ICT Office.

Once information is published on the worldwide web, anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on secured public web sites. All Internet usage from Mbhashe Local Municipality network is monitored and logged. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an investigation may result in action through Mbhashe Local Municipality's Labour Relations procedure and possibly criminal investigation.
Copyright and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Files so protected must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

8.11 Privacy of information, Private use, Legislation and Disciplinary Procedures

Information stored on a computer system or sent electronically over a network is the property of the individual who created it. Examination, collection, or dissemination of that information without authorization from the owner is a violation of the owner's rights to control his or her own property. Systems administrators, however, may gain access to user's data or programs when it is necessary to maintain or prevent damage to systems or to ensure compliance with other municipality rules.

Computer systems and networks provide mechanisms for the protection of private information from access. These mechanisms are not necessarily completely perfect and any attempt to circumvent them or to gain unauthorized access to private information (including both stored computer files and messages transmitted over a network) will be treated as a violation of privacy and will be cause for disciplinary action.

In general, information that the owner would reasonably regard as private must be treated as private by other users. Examples include the contents of electronic mail boxes, the private file storage areas of individual users, and information stored in other areas that are not public. The fact that that measures have not been taken to protect such information does not make it permissible for others to inspect it.

On shared and networked computer systems certain information about users and their activities is visible to others. Users are cautioned that certain accounting and directory information (for example, user names and electronic mail addresses), certain records of file names and executed commands, and information stored in public areas, are not private.
Nonetheless, such unsecured information about other users must not be manipulated in ways that they might reasonably find intrusive; for example, eavesdropping by computer and systematic monitoring of the behaviour of others are likely to be considered invasions of privacy that would be cause for disciplinary action. The

compilation or redistribution of information from the municipality directorates (printed or electronic) is forbidden.

8.11.1 Private use

Computing facilities are provided for Mbhashe Local Municipality's work and responsible personal use is allowed provided there is no conflict of interest with of the Municipality. The Municipality does not accept liability for any personal loss or damage incurred through using the Municipality's computing facilities for private use. Be advised that, in addition to violating Municipality rules, certain computer misconduct is prohibited by state law and is, therefore, subject to criminal and civil procedures.

Such misconduct includes:

- knowingly gaining unauthorised access to a computer system or database,
- falsely obtaining electronic services or data without payment of required charges
- intentionally intercepting electronic communications
- and obtaining, altering or destroying others' electronic information

8.11.2 Updates to this policy

In the light changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

8.11.3 Disciplinary action

Mbhashe Local Municipality wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it experts and supports the integrity of its employees. In exceptional circumstances, where there are reasonable grounds to suspect that employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Appendix 1 details examples of behaviour which is unacceptable within Mbhashe Local Municipality and provides examples of behaviour deemed as misconduct.

APPENDIX 1

Examples of illegal or Disallowed Actions (Misconduct):

- Visiting pornographic sites (adult top shelf materials) except where this forms authorised part of the employees job (for example "testing").
- Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.
- Obscene racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute.
- Downloading and installation of unlicensed products
- Viewing sexually explicit materials, except where this forms an authorised part of the employee's job.
- Chat rooms- sexual discourse, arrangements for sexual activity
- Violation of Mbhashe Local Municipality's registration with the Federation Against Software Theft – such as software media counterfeiting or illegitimate distribution of copied software.
- Frivolous use of the Municipality's computing facilities that risk bringing Mbhashe Local Municipality into disrepute. The distribution of animated Christmas card programme or "chain emails" beyond the internal e-mail system would represent examples of such misconduct.
- Entering into contracts via the internet that misrepresents Mbhashe Municipality. Contracts are legally binding agreements and an employee must not enter into any agreements via the internet to procure goods and services where Mbhashe Local Municipality is liable for this contract, without first consulting Mbhashe Local Municipality's financial procedures (available within the Finance department).
- Deliberate introduction of viruses to systems

This list is not exhaustive, but sets the framework of Mbhashe Local Municipality's approach to misuse of computing systems. Mbhashe Local Municipality has the right to monitor employees use of computer equipment where there is evidence to suggest misuse (Regulation of Investigatory powers Act 2000)

9. IMPLEMENTATION

2023/2024

10. REVIEWAL

Annually