NQUTHU MUNICIPALITY
UMASIPALA WASE NQUTHU
Private Bag X5521, NQUTHU, 3135
Tel: +27(0) 34 271 6100, Fax: +27(0) 34 271 6111

INFORMATION AND COMMUNICATION TECHNOLOGY USAGE POLICY

Policy Adoption Date:	13 DECEMBER 2018
Resolution Number:	C | 05 | 12 | 14
Authorised Signature:	

Table of Contents

1 DEFINITIONS

- **User** – refers to everyone who has access to the municipality ICT systems. This includes permanent employees, temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.
- **Information and communication technology (ICT)** - refers to the hardware, software and communications infrastructure used for information systems services. It encompasses all forms of technology used to create, store, exchange, communicate and use information in its various ways.
- **Information** – refers to data that is useful to a decision-maker. Any communication or representation of knowledge such as facts data or opinions in any medium or form.

2 LEGISLATIVE FRAMEWORK

This policy is established within the framework of the following legislation and regulations:

- Electronic Communications Act 36 of 2005
- Electronic Communication and Transaction Act 25 of 2002
- Protected Disclosures act 26 of 2000
- Promotion of Access to Information Act 2 of 2000
- Information Act 70 of 2002
- Municipal Systems Act 32 of 2000

3 OBJECTIVES

3.1 To regulate information and data security, including confidentiality, non-disclosure and non-solicitation.

3.2 To regulate authorised use of internet and email facilities and limited personal use.

4 APPLICABILITY

4.1 This policy applies to all employees of the Municipality including municipality managers and managers directly accountable to municipality managers in terms of section 56 of the Local Government: Municipal Systems Act 2000 (Act of 2000 as amended). It also includes Contractors and Consultants, who use ICT services and assets.

4.2 This policy applies to all equipment that is owned or leased by the municipality.

5 POLICY PRINCIPLES

5.1. The information technology and communications facilities should be used sensibly professionally, lawfully and consistently with the employees' duties with respect for colleagues and for the municipality and in accordance with the policy.

5.2. The information of clients and information regarding business conducted by the municipality must remain confidential and be treated with utmost care.

5.3. Many aspects of communication are protected by intellectual property rights which are infringed by copying, downloading, uploading, posting, copying, processing and distributing material from the internet without permission.

5.4. Particular care shall be taken when using email, internet message boards as a means of communication because all expressions of fact, intention and opinion in the email may bind the employee and the municipality and it can be produced in court as evidence.

5.5. All message sent on email system or via internet shall demonstrate the same professionalism as that which would be taken when writing a letter or fax.

5.6. Emails and internal notice boards should not be used to say anything that would subject the employee to disciplinary or legal action in any context such as sending discriminatory messages on the bases of a person's sex, race, disability, age, sexual orientation, religion or belief, defamatory, or unlawful material.

5.7. The employee must seek advice from a superior if there are doubts pertaining what needs to be done to ensure they do not violate the policy.

6 POLICY PROVISIONS

6.1 Use of Electronic Mail

6.1.1 General Provision

a) Always use the email template which contains the appropriate disclaimer notice from the municipality and do not amend this notice in any way.

b) If copying an email to others, it may breach legislation on data protection if reveals all the recipients email addresses to each recipient. It may be appropriate to use to Bcc (blind carbon copy) field instead of Cc (carbon copy)

field when addressing an email to more than one recipient. If in doubt the employee must seek advice from the seniors.

c) Do not amend any messages received except where specifically authorised by other person and does not access other person's inbox or other email folders, nor send any email in pretence that it comes from another person.

d) Proof read emails before sending.

e) Caution must be exercised when opening emails from unknown external sources where an email appears suspicious. ICT support should be informed immediately.

f) Employees shall observe and practice the bandwidth ranges and limitations provided by ICT from time to time.

6.1.2 Official Use

a) Each official email should include the appropriate municipality business reference.

b) When sending an important document always confirm that the messages has been received through telephone.

c) Back up any email as well as attachments that have been sent or received from a client before deleting the electronical copy. This also applies to all internal email communication.

d) In light of the security risk in some web-based email accounts, employees must not email official documents to their own personal web-based accounts. Employees may send documents to a client's web-based account if they have the client's express written permission to do so. Employees must never send highly classified information to the client's web-based email accounts.

6.1.3 Personal use

a) The municipality email is for official use, it is accepted that employees may occasionally want to use them for their personal purposes. When using the municipality email for personal use the employees must comply with all the rules and procedures of this policy. The employee must be aware that in using the municipality emails for personal use privacy will be compromised as the municipality will need to monitor communications when necessary.

b) Under no circumstances may the municipality emails be used in connection with operation or management of business that is not of the municipality or client of the municipality unless permission has been obtained from the superior in the municipality.

c) All the personal emails sent using municipality emails must be marked personal in the subject heading and must be filed in a separate folder which will be marked personal. Information communication and technology (ICT) support should be contacted to provide guidance on how to set up and use a personal folder.

d) Employees must ensure that their personal email use:
   i. Does not interfere with the performance of their duties.
   ii. Does not take priority over their work responsibilities.
   iii. Is minimal and limited to taking place substantially outside or normal work working hours.
   iv. Does not cause unnecessary expense and liabilities for the municipality.
   v. Does not have a negative impact in the municipality.
   vi. Does not contradict the municipality policy in any way.

e) The employee must be aware that the correspondence made using the municipality email might remain within the parameters of the municipality backups system even if the employee has deleted them as they would have been copied in backup tapes overtime.

f) By making personal use of the municipality email facilities for sending and receiving emails signifies the employee's agreement to abide by the conditions imposed for use and consent to municipality monitoring personal email.

6.2 Use of Internet and Intranet

6.2.1. An employee must be aware that when visiting a website, information identifying his/her PC may be logged. Therefore, any activity an employee engages on in the internet may affect the municipality.

6.2.2. The municipality recognises the need for employees to carry out some personal tasks during working hours, e.g. for internet banking or online shopping and this is permitted subject to the same rules as are set out for personal email use under this policy. If these activities require additional software to be installed onto an

employee's computer then a request should be submitted to ICT support who can assist within the confines of the policy.

6.2.3. Employees are discouraged from providing their municipality email address when using public websites for non-official purposes. This must be kept at minimum as this might result on the employee receiving substantial amounts of unwanted email in the municipality account.

6.2.4. Access to certain websites is blocked during normal hours. If an employee has a particular business needs to access such blocked sites, he/she should contact ICT support for permission of access.

6.2.5. An employee must not:

a) Introduce password detecting software.
b) Seek to gain access to restricted areas in the municipality's network.
c) Access or try to access data they know or ought to know is confidential.
d) Intentionally or recklessly introduce any form of spyware, computer virus or potentially malicious software.
e) Conduct hacking activities.
f) Use the municipality system to participate in any internet chat room, post messages on any external website, including a message board or blog unless it has been permitted in writing by the municipality.

6.2.6. Breach of the above would not only contravene the terms of this policy but could in some circumstances also amount to the commission of an offence under various legislation including:

a) Unauthorised access to computer material, i.e. hacking
b) Unauthorised modification of computer material
c) Unauthorised access with intent to commit or facilitate the commission of further offences

6.3 Misuse of facilities and systems

6.3.1. Misuse of the municipality facilities and systems including the telephone, email and internet systems is in breach of this policy and shall be treated seriously and dealt with in accordance to the municipality disciplinary procedure. Viewing, accessing, transmitting, posting, downloading or uploading any of the following material in the following ways or using any of the municipality facilities will amount to gross misconduct that may lead to dismissal:

a) Material which is sexist, xenophobic, homophobic, pornographic, paedophilic or similarly discriminatory and/or offensive.
b) Offensive, obscene or criminal material or material which is liable to cause embarrassment to the municipality, clients, other employees or bring the municipality to disrepute.
c) Any defamatory statement which is about any person or organisation or material which includes statements which is untrue or of deceptive nature.
d) Any material that is aimed at harassing the recipient.
e) Any material which violates the privacy of others or unfairly criticises or misrepresent others.
f) Confidential information about the municipality, employees and clients.
g) Statements which will create liability for the municipality (civil for the employee and / or municipality).
h) Material that may breach copywrite laws or intellectual property rights.
i) Gambling or commercial advertising material.

6.3.2. The municipality has a right to undertake a more detail investigation when suspecting a violation of the policy and shall take necessary disciplinary measures.

6.4 System security

6.4.1 The municipality must ensure that all official transactions are kept confidential. The municipality will need to demonstrate the credibility and integrity of the information contained in its ICT systems should it seek to use it court.

6.4.2 Municipality ICT systems and equipment must not be used in any way which may cause damage or overloading which may affect its performance or the performance of the internal and / or external network.

6.4.3 Employees must keep confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

6.4.4 Employees must keep the system password safe and manage them as per the instructions and guidelines issued by ICT support from time to time. Access to the user's inboxes must be authorised by the user. In cases where a password has been disclosed to another employee as requested by ICT systems it should be changed once that particular task has been completed.

6.4.5 A highly classified document should be marked by the employee as confidential and private and should be password protected.

6.4.6 Confidential information should be printed and retrieved from the printer immediately then stored safely or destroyed.

6.4.7 Employees should not take or copy the municipality software for personal use on their personal equipment.

6.4.8 No external devices or equipment should be run or connected to the municipality system without the prior notification to and approval of ICT support or superior.

6.5 Working Remotely

6.5.1 Employees who use municipality laptops and also use own computers equipment or other computer equipment whenever the employee is working on the municipality business away from the municipality premises must:

a) Password- protect any work which relates to the municipality business so that no other person can access the work;

b) Position himself/ herself such that their work cannot be seen by other people.

c) Take reasonable precautions to safeguard the security on the equipment and safeguard password(s).

6.5.2 The police and ICT support must be notified immediately if either a municipality laptop or any computer which contains municipality information and data has been lost or stolen.

6.5.3 Ensure that the work done remotely is transferred and saved in the municipality's system.

6.5.4 Pocket computers or smartphones or similar devices which may contain municipality information must be pass-word protected.

6.6 Personal blogs and websites

6.6.1 Personal content is content which is published by employees on the internet, blogs or social media that is created, updated, modified and /or contributions that are done outside of working hours and / or done using personal IT systems.

6.6.2 Employees are prohibited from publishing personal content during the working hours and/ or published using the municipality's systems.

6.6.3 If employees post any content on the internet which identifies or could identify them as employees of the municipality or they discuss their work, or anything related to the municipality or its business or its customers or personal or employees the

municipality expects them to behave appropriately in line with their contract of employment.

6.6.4 If an employee already has or intends to create a blog or website which indicates that he or she works for the municipality, he/ she should report to his or her line manager. If the blog clearly indicates that the employee works for the municipality, he or she must issue a disclaimer stating that "these *are my own personal views and not those of the municipality*"

6.6.5 The following will be treated as gross misconduct:

a) Revealing confidential information about the municipality in a personal online posting, such as revealing information relating to the municipality clients, business plans, policies, employees, financial information or internal discussions.

b) Online publications which share complaints about the municipality as an employer or a colleague, where the employee has not followed proper municipality procedures to raise that grievance.

c) If someone from the media or press contacts an employee about their online publications the employee responds without seeking guidance from the line manager and implicates the municipality.

6.7 Monitoring of Communications

6.7.1 The municipality is ultimately responsible for all business communications but subject to that it shall, as far as possible and appropriate, respect employee's privacy and autonomy while working. The municipality may monitor employees official communications for reasons including:

a) Providing evidence of business transactions;

b) Ensuring compliance to municipality's business procedures, policies and contracts;

c) Complying with any legal obligations;

d) Monitoring standards of services, employee performance and employee training;

e) Preventing or detecting unauthorised use of the communication system or criminal activities;

f) Maintaining the effective operation of the municipality communication system.

6.7.2 The municipality shall monitor telephone, email and internet traffic data (sender, receiver, subject, non-business attachments to email, numbers called and duration of calls, domain names of websites visited, duration of visits and files downloaded from the internet) at network level for the purposes specified above.

6.7.3 In cases where the municipality needs to access employee's emails while an employee is not at work or at their work station, access shall be granted only with the permission of one of the persons authorised to grant such access in accordance with the ICT support policy on access to mailboxes.

6.7.4 Emails which are stored in an employee's "personal" folder in their mailbox and which are not marked PERSONAL in the subject heading will be treated, for the purpose of availability for monitoring as business communication since there will be no way of knowing beforehand that they are personal emails.

6.7.5 All incoming email is scanned using virus-checking software. The software will also block unsolicited marketing emails and emails which have potentially inappropriate attachments.

6.8 Information and data protection

6.8.1. Whenever employees are processing personal data for the municipality they must keep it secret, confidential and secure and they must take particular care not to disclose that information and data to any other persons unless authorised to do so.

6.8.2. Employees shall not use personal data except as authorised by the municipality for the purpose of their work duties.

6.8.3. It is a criminal offence to obtain or disclose personal data without the consent of affected persons. Obtaining includes the gathering of personal data by employees at work without the authorisation of the municipality. Employees may be committing this offence if without authority of the municipality they exceed their authority in collecting personal data or access personal data held by the municipality, control it or pass it to someone else whether inside or outside the municipality.

6.8.4. Employees and former employees shall protect the confidential information and trade secrets, intellectual property and copyright of the municipality through:

a) Avoiding directly or indirectly divulging or disclosing confidential information;

b) Refraining from persuading clients or person who are or where suppliers of the municipality to cease doing business with municipality;

c) Refraining from soliciting business from service providers of the municipality;

d) Refraining from persuading employees of municipality to cease employment or take a different employment elsewhere.

7 ROLES AND RESPONSIBILITIES

The Municipal Manager or his /her nominee accept overall responsibility for implementation and monitoring of the policy.

8 DISPUTE RESOLUTION

Any dispute arising from this policy due to ambiguous wording or phrasing must be referred to the Local Labour Forum for adjudication. Resolutions from the Local Labour Forum shall be incorporated in the policy.