CAPRICORN DISTRICT MUNICIPALITY

EXTRACT FROM THE MINUTES OF COUNCIL MEETING HELD ON 29 JUNE 2017

ITEM

SC 13/2016-2017/5.1.5 **Reviewed Information and Communication Technology (ICT) Policies**

RESOLUTION

Resolved, That the following reviewed Information and Communication Technology (ICT) Policies be approved:

(a) Backup Policy;
(b) Data Centre Access Control and Environmental Policy;
(c) Change Management Policy;
(d) Notebook and Tablet Policy;
(e) Password Policy;
(f) ICT Account Management Policy;
(g) Electronic Mail Policy;
(h) Internet Policy;
(i) IT Security Acceptable Use Policy; and
(j) Municipal Corporate Governance of Information and Communication Technology Policy.

CERTIFIED AS A TRUE EXTRACT FROM THE MINUTES.

N.M. Lekganya

NM LEKGANYANE
COUNCIL SPEAKER

2017/06/29
DATE

CAPRICORN DISTRICT MUNICIPALITY
OFFICE OF THE SPEAKER
2017 -06- 29
LIMPOPO PROVINCE

CAPRICORN

DISTRICT MUNICIPALITY

RE ŠOMA LE SETŠHABA

SUBMISSION

Date: 26 JUNE 2017 **Memo Ref: 5/1/4**

TO : COUNCIL
DATE : 29 JUNE 2017
FROM : MAYORAL COMMITTEE
SUBJECT : INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICIES

1. PURPOSE

The purpose of the submission is to request Council to approve the review of Information and Communications Technology (ICT) policies.

2. BACKGROUND

The Municipality utilises data on a daily basis to perform its duties. This data needs to be effectively managed and secured to ensure that it is available as and when required. ICT and IKM unit has therefore implemented Policies to manage data, systems and access and to ensure effective use of ICT.

Some of these Policies were approved by Council and are now in the process of being reviewed.

The objectives of the policies are as follows:

Name of Policy	**Policy Objective**
ICT Backup Policy	The policy is aimed manage backup of data utilised by the Municipality. The policy outlines what data has to be backed up, how to store data and how to restore data
ICT Data Centre Access Control Policy	To manage access of the Server room and to ensure that physical conditioned of the server room is protected against fire and any other disaster.
ICT Change management Policy	To manage all changes done on all ICT systems. Changes are categorised in major

	and minor and relevant approval is required for every change.
ICT Notebook Policy	To manage the allocation, protection and the use of Municipal Laptops/Tablets
ICT Password Policy	To manage the use of passwords and password credentials, reset and unlock password.
ICT Account Management Policy	To manage the creation, modification and termination of user on the system
ICT Email Policy	To manage the use of email, the size of email and the language to be used when communicating through email.
ICT Internet Policy	To manage the use and access of Internet. It also list prohibited sites and restricted downloads
ICT Security Policy	To manage security and ensure that data is secured. It also outlines all security measures on the systems, infrastructure and network.
Municipal ICT Governance policy	To regulate Governance of ICT within the Municipality to ensure that ICT support Municipal strategies and that Municipal Council, Executive Management and Management plays a role in ICT initiative.

3. INPUTS FROM RELEVANT STRUCTURES

3.1 Inputs from Corporate Services Portfolio Committee

To include a table of policy number, date of approval, date of review by each committee on each policy so that the Municipality is able to easily track dates

3.2 Inputs from LLF Sub Committee (Basic Condition)

3.2.1 All Policies should be reviewed as and when required and not every two years.

3.2.2 Tablets for Councillors should be revised as follows:

- Provision of tools of trade for Councillors will be done in line with rules and regulations as determined by the upper limits and applicable legislation
- Wi-Fi access should be included in the policy.

4. RECOMMENDATION

That Council approves the reviewed Information and Communications Technology (ICT) policies.

CLLR M.J. MPE
EXECUTIVE MAYOR

2017/06/26
DATE

CAPRICORN
DISTRICT MUNICIPALITY

ELECTRONIC MAIL POLICY

Policy ref number: 10/5/P-2

DOCUMENT VERSION CONTROL			
Version	**Version Date**	**Nature of Change**	**Changed by Person**
1.0	07 August 2015	New Document	Corporate Services Department
1.1	25 August 2015	Review and Update	Executive Management
1.2	14 December 2015 09 May 2016	Review and Update	Management
1.3	29 March 2017	Review and Update	LLF Subcommitee
1.4	08 June 2017	Review and Update	LLF
1.5	19 June 2017	Review and Update	Corporate Services portfolio
1.6	26 June 2017	Review and Update	Mayoral
1.7			Council

TABLE OF CONTENTS

Appendices

1. Introduction

CDM provides Email facilities to all employees, contractors and service providers who utilize its network and/or network resources to enhance business operations, improve the sharing of information in an effort to accelerate service delivery to the public. CDM recognises that principles of freedom of speech, confidentiality and integrity of information have implications on the use of email facilities such that CDM has implemented Email content filtering systems to ensure that the use of Email facilities is in line with departmental requirements and objectives. This Policy reflects these firmly-held principles within the context of CDM's legal and other obligations. This Policy will be reviewed and/or amended annually from date of approval or whenever necessary.

2. Purpose of this Policy

The purpose of this policy is to:

i) Protect the integrity and public image of CDM
ii) Help boost productivity and prevent misuse of email facilities and network resources by clearly defining rules and restrictions for personal use
iii) Ensure that Email users are notified about the applicability of laws, regulations, standards, guidelines and best practices
iv) Ensure cost-efficient use of CDM email facilities and prevent monopolizing of resources
v) Assure that disruptions to CDM email facilities are minimized
vi) Ensure that Email users are informed on how concepts of privacy and security are applied to Email use

3. Scope

This policy applies to use of CDM email facilities or any emails sent via CDM internet facilities. It applies to all employees, vendors, and service providers operating on behalf of CDM. This policy only applies to electronic mail in its electronic form and it does not address printed copies of electronic mail.

4. References and Related Legislation and Regulations

The following publications govern the execution of the E-mail Acceptable Use Policy and were taken into consideration during the drafting of the email acceptable use guidelines and policy:

i) SABS/ISO 17799

ii) Information Security Forum (The standard of good practice for Information Security)

iii) Minimum Information Security Standards

iv) Copyright Act

v) Protection of Information act

vi) Promotion of Access to Information Act of 2000

vii) Public Service Act

viii) National Strategic Intelligence Act

ix) Regulation of Interception of Communications and Provisions of Communication-Related Information Act

x) COBIT Audit framework

xi) Electronic Communications and Transactions Act

xii) National Archives of SA Act 43 of 1996

xiii) International Standard for Risk Assessment

xiv) Limpopo Provincial Information Security Policy

5. Cautions

i) CDM will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that these systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, CDM can assure neither the privacy of an individual user's use of CDM's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

ii) The use of any CDM resources for electronic mail must be related to CDM official purposes. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for CDM. Any such incidental and occasional use of CDM E-mail facilities for personal purposes is subject to the provisions of this policy.

iii) There is no guarantee, unless authenticated mail systems are in use, that electronic mail received was in fact sent by the purported sender, since it is relatively straightforward, although a violation of this Policy, for senders to disguise their identity. Forwarded electronic mail can also be modified. If in doubt users should check with the purported sender or IKM support personnel to verify the authenticity of the message. Furthermore every email attachment should be scanned for viruses before being opened.

6. Policy Statement

E-mail users are expected to use CDM Email facilities responsibly, that is, comply with laws of RSA, other policies and procedures put in place by CDM, and with normal standards of professional and personal courtesy and conduct. Access to CDM E-mail facilities, when provided, is a privilege that may be wholly or partially restricted by the department without prior notice and without the consent of the email user when required by and consistent with the law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to CDM procedures or, in the absence of such procedures, to the approval of the Manager: IKM.

8.1 External Email Accounts and Instant Messaging

The use of external email accounts such as web mail, etc is not prohibited but for security reasons, email users are expected not to use these external email accounts to send, receive and store any official information and/or data. These email accounts are outside the control of CDM and as such their confidentiality, integrity and availability cannot be assured.

Instant Messaging applications such as MSN, Yahoo messenger, etc are prone to malicious code. More precisely, these applications can be used as entry points for viruses and worms into CDM's computer network. There are also confidentiality concerns with these applications and as a result Instant Messaging Applications other than those authorized by CDM are prohibited.

8.2 Prevention of Malicious Software

Emails are subjected to huge amounts of malicious software including viruses, computer worms and spyware. As a result, CDM has implemented technical measures to ensure that computer malicious software is prevented from entering the network and infecting computer systems. The following will govern incoming and outgoing malicious or potentially harmful attachments:

i) By default all virus infected mails will be blocked

ii) All attachments that cannot be scanned for viruses will also be blocked

iii) Typical virus hoaxes will be blocked

iv) All executable files or documents with embedded executables will be blocked. (Please refer to Annexure C for a list of prohibited executable files)

v) All unknown/unrecognizable attachments will be blocked

8.3 Communication of Official Information

Email users are expected to use CDM email facilities in accordance to departmental policies and procedures including but not limited to the communication policy. Only authorized personnel should distribute official information to both internal and external entities. This also means that in accordance with the communication policy, not everyone is authorized to send official emails to the All Staff Members and other distribution lists. Every branch shall select one member as the only authorized delegate to send emails official mails to distribution lists. These distribution lists must not be used for personal purposes, personal advertisements or distribution of junk mails.

8.4 Frivolous Use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Email users have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer/network resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, or distributing of large files, music, video files and creating unnecessary loads on network traffic associated with non-business-related uses of Email facilities. To minimize network load, an Email quota is set at 120 Megabytes.

8.5 Limitation of Privacy

Email facilities are provided to employees to improve information sharing and assist them in the performance of their jobs. Employees should acknowledge and understand the openness and privacy issues relating to the Email and as such have no expectation of privacy in anything they store or distribute using the CDM's Email facilities.

While CDM will put measures in place to ensure adequate Email security, users are cautioned that Email messages may be accessed and/or tampered-with by unauthorized third parties before reaching intended recipients. Additionally CDM Email content-filtering systems will automatically scan all incoming and outgoing emails to ensure policy compliance. If a policy breach is detected, the email message will be blocked and the sender or receiver of the message will receive a notification clearly indicating the conditions of the blockage to afford him or her opportunity to request the release of the message should the message be business related.

This request may be verbal through logging of a call with the IT Helpdesk or via email reply to the email message indicating policy breach. Authorized IKM personnel will only upon this request access the blocked email as to carryout further investigation. Thus by sending a message release request, the Email user consents IKM to access only the email message in question. Furthermore IKM personnel will not inspect the specific content of blocked email messages unless if the concerned contains a virus. For purposes of ensuring reliable Email facilities and diagnosing network problems GIKM staff may access the email history logs. These logs do not to reveal email contents.

8.6 Discriminatory, harassing and/or offensive language

Users are to refrain from using obscene, defamatory, derogatory, discriminatory or any offensive language while using CDM's internet facilities as such actions could have serious criminal, civil and moral consequences.

8.7 Monitoring and Reporting

It must be understood that CDM provides email facilities to all staff members primarily for work-related purposes. While personal use of email facilities is not discouraged, it can often lead to decreased employee productivity, misuse and violations of laws and regulations if not controlled. Therefore, IKM staff reserves the right to monitor email traffic from time to time for statistics, operation efficiency and reporting. This will ensure that IKM staff can predict email trends so as to proactively plan for future growth, continuously improve Email security and ensure compliance.

Mimecast solution has been implemented to secure and manage access to the email to protect from unauthorised use

8.8 Access to another employee's email

By default no employee except authorized IKM personnel is allowed to access another employee's emails or mailbox. If an email user requires another employee, (the delegate) to access his or her emails, then he or she must complete the Email Authorization Form **(Appendix A)** to IKM staff. IKM support personnel will not actively monitor employee mailboxes but it may be necessary for authorized IKM support personnel to view the contents of employees' electronic communications and Email activity or history in the course of problem resolution, system maintenance and operational duties. IKM support personnel may not view an employee's electronic communication out of curiosity or at the request of individuals who have not followed the correct authorization procedures.

8.9 Automatic Forwarding of Emails

Users are cautioned not to forward or create rules to automatically forward any official Emails to external email addresses such as web mail, mail accounts hosted by internet service providers, etc as this might result in disclosure of sensitive official information.

If an Email user leaves his or her employ at CDM or his or her services are terminated, IKM DEPT will at the request of the departing employee, forward all new incoming Emails to the Email address provided by the user. This is to ensure that the user will continue receiving important emails until he or she can notify contacts about the new email address. These emails will be automatically forwarded for a period of one month. To prevent intentional and unintentional information disclosures, all official emails will be exempt from this automatic forwarding.

8.10 Mailbox Limitations

All Email users have uniform quota limits set on their individual mailboxes of 120 (MB) **Megabytes**. Users close to their limit will be notified and the mailbox will be closed once this limit is exceeded. shall ensure that every user is aware of the different mailbox management methods including the use of personal folders and email archiving. In the absence or non-implementation of these mailbox management methods, email users shall ensure that they notify IKM support personnel for advice on mailbox management.

8.11 Email Retention and Archiving

E-mail users are notified that in accordance with the National Archives of SA Act 43 of 1996, all electronic messages will be archived for a period of 5 years.

8.12 Chain letters and Hoax and Spam emails

Users must not use CDM Email facilities to distribute chain letters, hoax and spam emails to other users. This is to ensure that Email resources are available to all legitimate users when necessary.

9. Prohibited Use

Prohibited uses of Email facilities include but are not limited to;

9.1 Distributing chain letters, junk mail and/or hoax email messages
9.2 Sending, receiving and storing of pornography and profanity
9.3 Sending, receiving and storing of audio and video files
9.4 Sending of emails to distribution lists to which you have not been granted the authorization
9.5 Sending of classified departmental information
9.6 Sending of emails of racial, hate, discrimination or sexist nature
9.7 Sending of unsolicited personal and commercial advertisements or promotions to other staff members or external email recipients
9.8 Sending of other people's confidential and personal information
9.9 Sending of data that violates copyright laws

9.10 Capturing and viewing of emails except when required for authorized IKM support personnel to diagnose and correct delivery problems as well as investigate policy breaches

9.11 Use of electronic mail to harass or intimidate others or to interfere with or deny other legitimate users the ability to effectively carryout their official duties

9.12 Use of electronic mail in any manner prohibited by national and international laws and regulations

9.13 "Email Spoofing" i.e. constructing emails so it appears to be from someone else

9.14 "Snooping" i.e. obtaining access to other people's emails for the purpose of satisfying curiosity

9.15 Attempting unauthorized access to electronic emails or attempting to breach security systems of any email system or "eavesdropping" i.e. attempting to intercept any electronic mail transactions without proper authorization

10. Disclaimer

All email messages sent from CDM's email facilities will automatically be stamped with the following disclaimer:

"The contents of this e-mail and any attachments are confidential. It is intended for the named recipient(s) only. If you have received this email in error please notify the sender immediately and do not disclose the contents to any one or make copies. Please note that the recipient must scan this e-mail and any attached files for viruses and the like. While we do everything possible to protect information from viruses, the Capricorn District Municipality liability of whatever nature for any loss, liability, damage or expense resulting directly or indirectly from the access and/or downloading of any files which are attached to this e-mail message. Opinions, conclusions and other information in this message that do not relate to the official business of the Capricorn District Municipality shall be understood as neither given nor endorsed by the said Capricorn District Municipality

11. Authorisation Procedures

11.1 A user will be granted access to email facilities upon completing an application for network access or signing an undertaking in the format **Annexure B,** through which, he/she will abide by the policy stipulations contained in this policy. This undertaking will be presented by IKM support personnel to the employee. The signed undertaking will be filled in the staff file of the employee. IKM support personnel will take all steps to ensure that all the employees are provided with these undertaking forms. Failure to sign shall lead to immediate revocation access to all email facilities.

11.2 In addition to signing the undertaking, a network logon message will be presented through which an employee will further agree to abide by the provisions and aspects of this Electronic Mail Acceptable Use Policy and any other relevant policy. This logon message will clearly indicate where the user can locate the policies for review. At this point the user will also be presented with an option to either agree to the policies by clicking the OK button or disagree by clicking the cancel button. Email resources will not be available to any user who does not agree to abide by and be legally bound by this Policy.

12 Responsibilities and Authority

12.1 Email User's Responsibilities

All Email users are responsible, accountable and liable for all their activities while using the departmental email facilities. As such the email user has the following responsibilities:

a) Ensure that their usernames and passwords are kept secure and not shared
b) Fully comply with all aspects of this policy
c) Immediately alert IKM support personnel about any misuse and non-compliance.
d) Duty not to waste computer/network resources
e) Continuously protect the integrity and public image of CDM

12.2 IKM support personnel's Responsibilities

IKM support personnel is responsible for the following:

a) Implement technical measures to ensure adequate Confidentiality, Availability and Integrity of CDM email facilities
b) Monitor and enforce policy compliance
c) Follow appropriate channels to resolve policy breaches and incidents
d) Educate Emails users whenever possible about Email security best practices and this Electronic Mail Acceptable Use Policy.

13. Consequences of Non-Compliance

All CDM employees, contractors or temporary staff who have been granted the right to use the CDM's Internet access are required to sign this agreement confirming their understanding and acceptance of this policy. All employees, contractors or temporary staff who have been granted the right to use the department's email facilities are required to sign the internet and email user undertaking confirming their understanding and acceptance of the policies. As already stated, non-compliance of this policy may lead to disciplinary actions, legal liability as well as all email privileges for the user in violation revoked

14. POLICY REVIEW

This policy will be reviewed as and when required

15. APPROVAL

This policy was approved by ___________________ on the _______ day of _________ 2017