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.

NM LEKGANYANE
COUNCIL SPEAKER

2017/06/29
DATE

CAPRICORN

DISTRICT MUNICIPALITY

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.

2017/06/26

CLLR M.J. MPE
EXECUTIVE MAYOR

DATE

P140

CAPRICORN

DISTRICT MUNICIPALITY

INTERNET POLICY
Policy Reference number: 10/5/P-1

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

P141

TABLE OF CONTENTS

1. PREAMBLE

The World Wide Web is a worldwide network of computers that contains millions of pages of information. The internet is a necessary job-enhancing tool because it allows internet users access to information required to carryout and enhance their jobs when required. Recognising the importance of the internet, many organisations and government departments have implemented information systems to provide staff members with access to the internet.

However, an organisation which connects its networks to the internet exposes its information systems to all kinds of internet-borne security risks due to the open nature of the internet. Furthermore, current-day applications like e-mail, www, etc require relatively large amounts of bandwidth, of which the demand and cost is very high. As a result organisations connected to the internet need to implement technical and procedural measures to mitigate risks from untrusted networks and to ensure that internet resources are utilized in a manner which does not adversely impact normal business operations.

2. INTRODUCTION

CDM provides internet and World Wide Web access to all its employees and employees are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the internet. Even harmless search requests may lead to web sites with highly offensive and/or malicious content. Additionally, having a web-based email account on the internet may lead to receipt of unsolicited e-mail containing offensive and malicious content.

While CDM implements adequate measures to govern internet usage, employees are ultimately responsible for any internet-related activities and any material viewed or downloaded by users from the Internet. To minimize these risks, the use of the Internet facilities at Capricorn District Municipality is governed by this Internet Acceptable Use policy.

3. Objectives of this Policy

The objectives of this policy are:

i) To define security "laws and governance" that shall be enforced departmental wide to ensure that CDM internet information systems are adequately protected from misuse or direct/indirect exposure to security risks

ii) To ensure the highest possible level of Confidentiality, Availability, Reliability and Integrity for the CDM network, Information and information systems

iii) To encourage cost-effective and productive use of CDM internet systems

iv) To clearly define user responsibilities and liability when using departmental internet facilities in day-to-day activities

v) To ensure compliance with regulations of RSA and other relevant international laws, regulations, standards and best practices

4. Application of this policy

This policy applies to all employees (including service providers, contractors and temporary staff) utilizing Municipal internet systems via 3G data cards, municipal computers and laptops as well as CDM networks.

5. References and Related Legislation and Regulations

The following publications govern the execution of the internet use policy and were taken into consideration during the drafting of the internet use guidelines and policy:

i) SABS/ISO 17799
ii) Minimum Information Security Standards
iii) Protection of Information act
iv) Public Service Act
v) National Strategic Intelligence Act
vi) Regulation of Interception of Communications Act
vii) COBIT Audit framework
viii) Electronic Communications and Transactions Act
ix) International Standard for Risk Assessment

6. Policy Statement

Internet users are expected to use CDM's internet facilities in a responsible manner which complies to the laws and regulations of RSA, other international laws as well as policies, standards and guidelines as set by CDM. Access to CDM's internet facilities is a privilege that may be wholly or partially restricted by the department without prior notice and without the consent of the internet 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 Municipal Manager of CDM.

6.1 Methods of Connecting to the Internet

To ensure security and avoid the spread of viruses and other security threats, Users accessing the Internet through a computer attached to CDM's network must do so through the municipal information security systems like firewalls, Intrusion Prevention Systems, etc. Every employee will use his or her network username and password to access the internet for accountability and reporting purposes.

Bypassing CDM's computer network security by accessing the Internet directly by modem, 3G cards, mobile phones connected to computers, non Departmental wireless networks or other means is prohibited unless prior arrangements with IKM support personnel is made and subjected to approval by the IKM Manager.

6.2 Detection of Viruses

Files obtained from sources outside CDM, including fixed and/or removable disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by vendors, may contain security risks that may damage CDM's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-CDM sources, without first scanning the material with CDM-approved virus checking software. If you suspect that a virus has been introduced into CDM's network, notify Manager IKM immediately. If you are uncertain how to scan for viruses immediately contact IKM support personnel for assistance.

6.3 External Email Accounts and Instant Messaging

While external web mail accounts are not disallowed, users must ensure that these email accounts are not used to distribute and/or store official information as this might lead to intentional/unintentional disclose of sensitive official information. Only departmental email systems must be used when distributing official information.

Due to high number of security risks associated with Instant Messaging applications line msn messenger, yahoo messenger, etc users are not allowed to use and install any instant messaging application on departmental computers or networks.

6.4 Distribution of information and data

Without prior written permission from CDM, the CDM's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, trojan horse programs, etc.) or any other unauthorized materials. Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the users or any other employee's job performance; b) have an undue effect on the computer or CDM network's performance;) or violate any other policies, provisions, guidelines or standards of this agreement or any other of CDM. Further, at all times users are responsible for the professional, ethical and lawful use of the departmental internet facilities.

6.5 Communication of Official Information

Unless expressly authorized to do so, users are prohibited from sending, transmitting, or otherwise distributing official information, data or other sensitive/confidential information belonging to CDM through the World Wide Web. Unauthorized dissemination of such material may result in severe disciplinary action and other appropriate actions under the laws and regulations of RSA or any international laws.

6.6 Discussion Groups and Social media

6.6.1 No CDM employee may in his/her official capacity create, participate in discussion groups on the internet and Intranet. No offensive, racist or any messages containing vulgar language is to be send to employees. Also, do not use the e-mail system to as a discussion group to insult colleagues or to discredit others.

6.6.2 Social media will only be accessed outside working hours.

6.7 Copyright Restrictions

Users may not illegally copy material protected under national and international copyright laws or distribute that material to other people. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not under official duties agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the IKM support personnel.

6.8 Frivolous Use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all internet 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, spending excessive amounts of time on the Internet, playing online games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, accessing P2P networks/applications or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

To ensure reliable network connectivity and faster access to the internet, a limit for access and downloads may be set per user.

6.9 Limitation of Privacy

Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should acknowledge and understand the openness and privacy issues relating to the internet and as such have no expectation of privacy in anything they store or distribute using the CDM's internet facilities.

User consents to allow authorized IKM support personnel to access to and review of all materials created, stored, sent or received by User through municipal Internet facilities for the purposes of accounting, monitoring of policy compliance and internet usage statistics. Web security allows IKM support personnel to view the sites visited by officials and if they find the sites being offensive, the site will be blocked and a blocking message will appear to contact system administrator to unblock the site if the user motivates for a need to access the site for official purposes. Regular offenders will be reported to their Departmental Manager.

6.10 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.

6.11 Installation and Downloading of Software

Recognizing the many security risks on the internet, users are cautioned not to install or download any software from the internet as this might result in copyright violations, virus infections, and installation of hardware, spyware and malicious monitoring software. Opening malicious web sites can often lead to automatic installation of malicious software and users are also cautioned not to agree to any automatic installation presented by web sites.

If a user is uncertain about how to proceed, it is his or her responsibility to get advice from IKM support personnel. A user knowingly downloads and installs any software from the internet that can compromise the CDM network, information systems or those users will be in violation of this policy.

6.12 Additional Connections to the Internet

The Municipality offers additional tools like 3G data cards to selected employees to help enable remote internet connection and access to emails from remote locations. It must be understood that the usage of these 3G cards are governed by this Internet Acceptable Use Policy and as such 3G data cards users must ensure that they utilize these 3G cards for official purposes. 3G users are more vulnerable to virus attacks and other security risks from the internet as they are not protected by departmental information security systems. This means that a 3G user visiting malicious sites could unknowingly distribute security risks to other computers while connected to the CDM network.

To exercise control over security risks and maintain a single point of internet connection, all users connected to the municipal network are not allowed to connect their 3G cards. Additionally the use of 3G cards applies only to users at remote locations. 3G cards are only intended for internet access and they shall not be used for any other purposes like making phone calls.

No internet user is allowed to configure or enable other connections to the internet via modems, wireless networks and cell phones on municipal computers. Any additional internet connections should be reported to IKM support personnel.

6.13 Monitoring and Reporting

CDM accepts that the use of the Internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the municipality. In addition, all of the municipality's Internet facilities are provided for primarily official purposes. Therefore, the municipality maintains the right to monitor and log the volume of Internet and network traffic, including but not limited to Internet sites visited, files downloaded by users, etc.

The specific content of any transactions will not be monitored unless there is a suspicion of improper use or policy violation. It may also be necessary for authorized IKM support personnel to view the contents of employees' electronic communications and internet activity history in the course of problem resolution. IT 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.

7 Prohibited Use

7.1 Accessing streaming audio or video, play online games unless if it is for official use
7.2 Accessing chat sites unless if it is for official use
7.3 Installing and using instant messaging applications
7.4 Download of copyrighted material including videos, music, software or any intellectual property
7.5 Accessing web sites and material that may be offensive to other employees. This includes but not limited to pornography, hate speech web sites, criminal/illegal activities, etc
7.6 Using the internet to conduct criminal or fraudulent activities
7.7 Using the internet to illegally monitor, gather information about any individual, entity or organization.
7.8 Using the internet to intentionally subvert security systems or initiate a denial of service against any information system or network
7.9 Using the internet to conduct any personal business operations at the expense of the department's bandwidth and resources
7.10 Using the internet such that it interferes with employee productivity
7.11 Sharing of usernames and passwords of other official to access the internet
7.12 Distributing of passwords or any sensitive user account information through the internet
7.13 Impersonating, misrepresenting or suppressing a user's identity when accessing the internet
7.14 Using the municipal internet facilities to intercept or disclose, or assist in intercepting or disclosing municipal electronic data or information.
7.15 Using profanity, obscenities, sexist, racist, highly sensitive, offensive or defamatory remarks while using the internet.
7.16 Using the internet to access malicious sites and download illegal material

8. Conditions for internet Access

An employee must sign and accept the conditions and liabilities of this internet acceptable use policy before being granted access to the network. If the internet user then violates any part of this policy, remedial actions such as revoking the user's internet access and/or disciplinary may be taken. Depending on the outcome of the investigations the user may be required to reapply for internet access by filling in the relevant forms.

9. Authorisation Procedures

For purposes of ensuring proper use accountability, control and proper use of the Internet, every employee utilizing a municipality notebook, computer, 3G card shall sign 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. 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 existing internet access for that employee revoked.

10. Responsibilities and Authority

10.1 Internet User's Responsibilities

All internet users are responsible, accountable and liable for all their activities while browsing the internet. As such the internet 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 Manager-IKM about any misuse and non-compliance.

d) Duty not to waste computer/network resources

e) Understand that the information or data sent via the internet may/can be intercepted by other individuals and ensure that they fully acknowledge this privacy concern.

11. Implementation and monitoring

The Municipality is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

12. Consequences of non-compliance

Non-compliance of this policy will lead to disciplinary action, taken against an official.

13. Policy review

This policy shall be reviewed as and when required.

14. Approval

This policy was approved by council on the ....day of ....

Signed by ....in his/her capacity as ....

On behalf of council, on the ....of...............................