

EMAKHAZENI LOCAL MUNICIPALITY



INTERNET POLICY

Approval

DOCUMENT:	INTERNET POLICY		
Copy Number:	Master Copy		
Compiled by:	Niall Carroll	Reviewed by:	
Compilation Date:	August 2013	Review Date:	
Version:	V 1.03	Revision:	
Distribution:	All	Classification:	
Document Release Approval		Document Acceptance	
Releasing Authority: Deputy Manager: ICT	ICT	Acceptance Authority:	Council
Date Released:		Date Accepted	
	Signature:		Signature:

DOCUMENT CONTROL

0.1 Revision Record

Revision	Date	Change Record	Changed By
1 st		Revised ICT Policy – Submitted to Council	N Carroll ICT
2 nd	March 2 0 1 3	Reviewed and updated	N Carroll ICT
3 rd	August 2 0 1 3	Re formatted layout	N Carroll ICT

0.2 Issue Control

This policy is issued by the Corporate Services Department on behalf of Emakhazeni Local Municipality, to whom any change requests or queries should be directed. The review life for this document is 12 months.

0.3 Distribution

Copy No.	Name	Title	Organisation
Master			
01			
02			

The MASTER for this document is held electronically and only signed copies are valid. An unsigned, printed document is not copy controlled and is to be used for information

purposes ONLY, as it will not be automatically updated. It is therefore the responsibility of the reader to ensure that it is a currently valid copy.

Table of Contents

DOCUMENT CONTROL 3

0.1 Revision Record..... 3

0.2 Issue Control..... 3

0.3 Distribution 3

INTERNET POLICY 6

PURPOSE OF THE POLICY 6

INTERNET USAGE 6

INTERNET PUBLISHING 8

PURPOSE OF THE POLICY

The purpose of the policy is to assist in the control of and access to the Internet and the publishing of information.

1. INTERNET USAGE

The use of the Internet is subject to the relevance of it to the employee's job function and work. The government does not allow access to sites that are not work related or that can degrade the service and image of the government locally, provincially or nationally. All Internet sites accessed must be work related as far as possible. The Internet should be used as a tool to promote the image and responsibilities of the municipality and to ensure that it can provide a better service to the whole community.

The government has through criticism and in some cases laws directed that the following sites are not to be accessed from government computers as to protect the government against such criticism:

- Web sites that contains nudity of any type (hard core, soft core, sex or other pornographic content not mentioned specifically, including so-called art oriented nudity)
- Web sites that promote or display any type of nudity, sexual actions and graphics of children and persons considered children under the laws of the country. Where this instruction is ignored the person opens himself/herself not only to departmental Disciplinary action but also to criminal prosecution.
- Web sites that displays violence to promote violent behavior or attempt to disgust and/or upset members of staff and the public visiting the offices
- Web sites with content that promotes action against the government or organizations that are protected under government laws
- Web sites that promotes propaganda against any person or group of persons that are protected by law
- Web sites that seeks to discredit any organization, statutory or private
- Web sites that allows for the use of government computers to perform illegal actions such as distribute software or music for example Kazaa and other similar sites where information is illegally shared over the Internet

- Web sites that has the aim of illegally accessing the user's computer or gain network access where the user works
- Web sites that enables the user to play games online and that will abuse available bandwidth to such an extent that the normal work of employees are negatively affected
- Web sites where people can communicate socially over the Internet in chat rooms or using a client to enable such actions like Facebook, UTube, Twitter, MSN Messenger, Yahoo! Buddy, etc.
- Web sites that deals in illegal products or content

The management of the municipality has discussed and agreed that the use of the Internet for sites not belonging to any of the above-mentioned criteria and that is not work related will not be prosecuted provided that visiting such sites does not negatively affect the operation of the person and/or department. This is where Internet services are available at present. New installations will not be granted on the premise of accessing the Internet because of the above-mentioned statement. The government laws and direction should in all cases still be adhered to and applied to ensure good governance and control over government funds and time. Internet access will not be allowed where a job function does not allow such access.

All users may have access to the Intranet of the municipality or other Intranet agreed upon by management of the municipality. Access to the Internet is only granted on application where such access is necessary for the completion of tasks for such members of staff.

Users of the Internet are not allowed to download music in any format, movies or any software that are deemed licensed software for personal use and or retail purposes. This is in direct contravention of copyrights and anti-piracy laws internationally and can open the official to criminal prosecution. No user may utilize government equipment for such actions. This includes using government issued compact disk rewriters (CD-RW) to reproduce music or movies for any reason, including but not limited to personal use or retail of such content. This will also include reproduction of such content for official use where no explicit authorization was granted or obtained for the reproduction of such content to benefit the department or organization. Where it forms part of a presentation that aims not to discredit but educate without contravening the copyright of such content but rather enhance the organization or department without having the content as the main focus such content may be recorded for use by the relevant personnel only. Where such content is to be used publicly, the necessary authorization must be obtained for the use of such content.

Users with Internet access may not have any or all of the following applications installed on their workstations/computers as it abuse available bandwidth and can be used to defeat security systems and software in place:

- MIRC
- ICQ
- Yahoo! Buddy/Companion
- MSN Messenger
- AOL Companion
- BonziBuddy

Any other IRC-related application not mentioned here, except that which may be allowed by management that will be part of communication packages in place on the network such as a relay agent shipping with programs such as GroupWise, MS Outlook and MS Exchange. Such programs are guaranteed as secure communications by their owners and will not aim to defeat the security systems and software installed and implemented on the network. The mentioned applications have been found to carry intruders successfully into secure environments and can disrupt network operations and cause downtime or add to the distribution of computer viruses.

2. INTERNET PUBLISHING

All content to be published on the Internet must be authorized before it is published as information that are considered sensitive may result in public uproar and action against the department or municipality. No information may be published without the authorization of the office manager or his/her delegate.

The publishing of information on the Internet should be done only by one person or institution or company to avoid duplication of tasks and to ensure accuracy of information. This will ensure that only relevant information is published on the Internet and that information has been cleared through the relevant channels to be published. If outside personnel do the web publishing then it is imperative that one person be appointed to liaise with the company, person or organization responsible for publishing the information to ensure that all work done are according to the wishes of the municipality or department.

The publishers of information should ensure that the server being used is secure and properly protected against illegal outside access. No web page published on Microsoft Internet Information Server should be considered safe and extra precautions should be taken to safeguard the server against illegal outside access. The Internet Information

Server and all upgrades there-of has been shown to have security issues and allow illegal access to the server and network.

The information that should be published and be publicly available according to government laws should be made available on the web page for all Internet users to see and access. This should also be published on the Intranet page to ensure that it is accessible to all.