EMAKHAZENI LOCAL MUNICIPALITY

E-MAIL POLICY

Approval

DOCUMENT:	**EMAIL 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
1st	April 2009	New ICT Policy – submitted to Council	N Carroll ICT
2nd	March 2013	Reviewed and updated	N Carroll ICT
3rd	August 2013	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

1. E-MAIL USAGE

1.1. Electronic mail or e-mail should be seen as a privilege and not a right. It is therefore imperative that the user should ensure that his/her e-mail access is kept official and at all times devoid of profanity, obscene, racist, defamatory, abusive or threatening, discriminatory or otherwise biased remarks or content, lies to discredit the municipality or any individual that acts as representative of the municipality or government and propaganda to discredit any person or group of people or party in any way.

1.2. Emakhazeni local Municipality email is issued to employees to correspond with clients and public. It is the official e-communication of the Municipality. The use of private emails, Gmail, yahoo, msn, hotmail, etc., for official Municipal correspondence is not accepted in any form. This can compromise the principles of good governance and validity of the mail sent to the client.

1.3. Municipal computer users should also not distribute or forward any content that is sexual, pornographic, biased, offensive or violent to disgust or that can be viewed as inappropriate or illegal content. The principles of good governance should at all times be adhered to and practiced without exception.

1.4. All e-mail messages that consist of files that are copyrighted and therefore illegally distributed via e-mail are deemed illegal and steps can be taken not only disciplinary but also in a court of law against offenders. It is also illegal to send information that is derogatory to any person or messages of sexual harassment via e-mail to any person, either within the municipality or outside. It is also illegal to read any e-mail message intended for a specific person, unless specifically instructed or requested to do so.

1.5. Where people allow other access to their e-mail messages it should be noted that permission is given to read messages received via e-mail and therefore it is not deemed illegal to read any message received.

1.6. People making use of proxy connections to other personnel's mailboxes should therefore rather be appointed in writing to accept and read e-mail on behalf of the person.

1.7. It is also deemed illegal to send e-mail that contain user accounts and passwords to persons not on the network or not members of the network, especially if those accounts and passwords grant access to the network with administrator or equal rights and the intended party uses it illegally. When

instructed to do so such information may be sent via e-mail but only on instruction by a member of senior management. All users should note that in some cases the steps that can be taken include jail terms and such actions may be criminal and will be prosecuted to the fullest extent of the law as to show a no mercy towards public officials abusing the privileges they have at the work place and to show a firm stance against criminal elements in the community.

1.8. E-mail users should not distribute any e-mail that can harm the network of Emakhazeni local Municipality or any other government organization or department or private network. Distributing such programs or content can be viewed as sabotage and relevant proceedings may be entered into against the person.

1.9. It is important to note that the government will under no circumstances protect an individual or group of individuals that do not adhere to the laws of the country or disobey any instruction, written or verbal, to ban certain activities or actions. People that do make themselves guilty of such actions will face prosecution and may have to serve jail terms for such actions.

1.10. All e-mail messages should be kept to a maximum size of about 2 megabyte or less. This will aid in the necessary bandwidth being conserved and utilized for important transfers.

1.11. Users are also requested to keep private e-mail to the absolute minimum and all users are hereby informed that on all government networks monitoring software may be installed and used to monitor all electronic communications in accordance with the Intelligence acts and to ensure that the country is properly protected against terrorism of any type.

1.12. Although there is an act that states that e-mail messages may not be monitored it is not the case on a government network as it is a public network with access points into the intelligence centers of the country and it should therefore be protected. The only provision is that content may not be made public if it is not considered a threat but statistics can be used for non-performance of officials where applicable. Then larger e-mails are to be sent or received the support personnel should be contacted and informed as to ensure that the message is properly uploaded or downloaded and not discarded by the system.

1.13. Mail systems today are commonly configured to receive mail messages of a predetermined maximum size only and e-mail messages, whether work related or not that exceeds that size are immediately discarded. Notifying the support personnel will ensure delivery or receipt of the needed information via e-mail.

1.14. Users are allowed to use any e-mail client to send or receive information provided that the program is accepted and supported by technical support staff or the company employed to perform such tasks. The user should also note that onlythe authorized e-mail clients would be supported and no other.

1.15. Users may not send out virus warnings if it was not cleared with the relevant support person or company. Users should not send out such forwarded messages as it is usually hoax viruses that aim to flood e-mail systems and servers through sheer volumes than propagating itself. Such mails are usually not stopped by mail monitoring software as it does not contain viruses but acts as viruses and have a similar effect.

1.16. Users that distribute computer viruses via e-mail may be held responsible for charges in ridding the system of such computer viruses, especially if it was sent knowingly that such e-mail contained a computer virus or viruses.

1.17. Users should inform the support personnel or company of any strange content or e-mails received from known and unknown sources, especially when the mails contain attachments that are executable files or part of applications or application extensions or even screensavers. Such attachments may be disguised computer viruses and may wait to be executed to infect a system and redistribute it to other recipients. E-mails received from unknown sources or that is conspicuous by nature should be deleted immediately and also deleted from the recycle bin within the e-mail program.

1.18. Other known and quite often-received viruses comes in the form of Word documents or even Excel spreadsheets and are macro viruses that negatively affect the Word or Excel applications. These viruses can damage documents and files that are opened and corrupt it to such an extent that the information contained there in is lost.

1.19. All users must make sure of the security classification of documents sent via e-mail and ensure that the documents may be sent via e-mail. Where documents are sent with sensitive information the relevant support personnel should be contacted to ensure that the mail is sent encrypted and that sensitive information is received by the intended recipient only and can be read by that person only. Encryption is a way to send information securely via an e-mail system without the fear of being read by people that should not have access to such information.

1.20. E-mail should as far as possible not be allowed to accumulate on the file server as to conserve disk space and ensure proper use of the file server.

1.21. The municipality's Internet Service Provider is required to keep e-mail and/or headers for a specified time. The timeframe is yet to be fixed and it could come down to the organization to hold such information for a specified period. This is required by law and should be considered when accumulating e-mail and other data on file servers

1.22. A formal instruction will be issued to inform of such actions to be taken. This will be in accordance with the intelligence and information availability acts of the country.

1.23. No e-mail message intended for a user may be published unless instructed to do so for the sake of feedback to members of staff of the department or municipality as a whole