



NDLAMBE MUNICIPALITY

DRAFT

INTERNET, INTRANET, EXTRANET AND E-MAIL POLICY

21 FEBRUARY 2007

Table of Contents

1. PREAMBLE.....	5
2. GENERAL DEFINITIONS AND MEANING OF TERMS.....	5
3. POLICY OBJECTIVES.....	5
4. SCOPE OF POLICY.....	6
4.1 INTERNET.....	6
4.2 INTRANET.....	6
4.3 EXTRANET (SPECIALISED DIRECT LINKS).....	6
4.4 E-MAIL.....	6
5. OWNERSHIP.....	6
6. REVIEW.....	7
7. IMPLEMENTATION.....	7
8. ROLE PLAYERS.....	7
9. POLICY STATEMENTS.....	8
9.5 UNACCEPTABLE USES OF THE INTERNET AND NDLAMBE MUNICIPALITY E-MAIL:.....	8
9.6 ACCEPTABLE USES OF THE INTERNET AND NDLAMBE MUNICIPALITY E-MAIL:.....	9
9.7 ARCHITECTURE AND INFRASTRUCTURE:.....	9
9.8 ADHERENCE.....	9
9.9 SECURITY (SEE ALSO SECTION 12).....	10
9.10 OUTSOURCING.....	10
10. VIOLATIONS AND PENALTIES.....	11
11. OFFENCE/CATOGORY.....	11
12. ELECTRONIC MAIL SECURITY.....	13
12.1 MUNICIPAL PROPERTY:.....	13
12.2 AUTHORIZED USAGE:.....	13
12.3 DEFAULT PRIVILEGES:.....	14
12.4 USER SEPARATION:.....	14
12.5 USER ACCOUNTABILITY:.....	14
12.6 USER IDENTITY:.....	14
12.7 NO DEFAULT PROTECTION:.....	14
12.8 RESPECTING PRIVACY RIGHTS:.....	15
12.9 NO GUARANTEED MESSAGE PRIVACY:.....	15
12.10 REGULAR MESSAGE MONITORING:.....	15
12.11 STATISTICAL DATA:.....	15
12.12 INCIDENTAL DISCLOSURE:.....	15
12.13 CONTENTS OF MESSAGES:.....	16
12.14 MESSAGE FORWARDING:.....	16
12.15 HANDLING INFORMATION ABOUT SECURITY:.....	16
12.16 PUBLIC REPRESENTATIONS:.....	16
12.17 USER BACK-UP:.....	16

12.18	ARCHIVAL STORAGE:	17
12.19	PURGING ELECTRONIC MESSAGES:.....	17
12.20	HARASSING OR OFFENSIVE MATERIALS:.....	17
12.21	ACCESS TO INTERNET E-MAIL:	17
12.22	VIRUS SCAN OF E-MAIL:	17
13.	STANDARD E-MAIL DISCLAIMER	18

1 PREAMBLE

The growth of the Internet and E-mail as primary communications channel is increasing every year. The Internet and e-mail provides access to information and services that would previously been very difficult to obtain. In addition, National and Provincial Government are encouraging the use of the Internet as a means to improve the accessibility of government services to all.

By providing organisations and employees access to the Internet and e-mail in the normal course of their daily duties increases the risks faced by organisations on multiple levels. The security of the Municipal systems and information must be ensured at all times. The Internet greatly increases the risk of security breaches, theft of confidential information and incidental or unintentional disclosure of confidential information, which can result in legal proceedings by the aggrieved party.

Furthermore, in a similar way that the telephone improved communications, but was also subject to wide spread abuse by employees, so too can the Internet and e-mail be subjected to abuse. The cost of which must be borne by the municipality in terms of cost and loss of productivity. The intention of an e-mail policy is to provide guidelines for the use of the electronic media and where abuse occurs, sets out the punitive measures that can be taken against an employee. The Internet and E-mail policy also controls the content that can be accessed over the Internet and prohibits the transmission of harassing and sexually explicit material.

The Internet and e-mail policy also specifies the security measures and safeguards that should be applied by the IT department and the employee alike.

2 GENERAL DEFINITIONS AND MEANING OF TERMS

- 2.1 The term "NDLAMBE Municipality" includes the NDLAMBE Municipality with all its Departments.
- 2.2 The group term "Internet" includes Internet, Extranet, Intranet and e-mail services. Where a specific word, such as e-mail, is used it is for clarification and does not necessarily exclude the others of the grouping.

3 POLICY OBJECTIVES

This policy shall:

- 3.1 Indicate NDLAMBE Municipality's requirements and standards regarding the implementation, usage, management and administration of Internet access.
- 3.2 Demarcate the roles and responsibilities of participating organisational Units.
- 3.3 Promote awareness among NDLAMBE Municipality Internet users regarding the procedures, costs and risks involved in accessing the Internet.
- 3.4 State NDLAMBE Municipality's position in the event of non-compliance with the Internet policy by any NDLAMBE Municipality Internet user.
- 3.5 Define guidelines, standards and procedures for NDLAMBE Municipality divisions providing information or services on the Internet.

4 SCOPE OF POLICY

The scope of this policy shall be bound by the controlled and secure usage of NDLAMBE Municipality's infrastructure and supplied Internet channels by NDLAMBE Municipality and its clients and shall include:

4.1 Internet

The NDLAMBE Municipality Internet shall be used as another delivery channel to offer communication and information to NDLAMBE Municipality constituents and potential constituents and, work related World Wide Web (WWW) access for NDLAMBE Municipality employees.

4.2 Intranet

The NDLAMBE Municipality Intranet is devoted to NDLAMBE Municipality's departments and/or business units to make internal communication more efficient and effective.

4.3 Extranet (Specialised Direct links)

The NDLAMBE Municipality Extranet, or extended Internet, shall be used by NDLAMBE Municipality to form a tight electronic communications channel relationship with its government structures or the private sector in the case of e-procurement and e-governance.

4.4 E-mail

The NDLAMBE Municipality supplied e-mail service is to make both external and internal work related communication more efficient and effective. Both internal and externally based browser (for example "Hotmail.com") and client (for example "Microsoft Outlook") e-mail shall, if accessed by using NDLAMBE Municipality's infrastructure and supplied Internet channels, be deemed to be governed by this policy.

5 OWNERSHIP

- 5.1 NDLAMBE Municipality is the owner of the policy.
- 5.2 NDLAMBE Municipality Information Technology (IT), or the department responsible for IT, will execute and coordinate the maintenance of the policy in consultation with relevant parties.

6 REVIEW

The policy must be reviewed at least annually. Any proposed interim alterations must be tabled via the NDLAMBE Municipality IT, or the department responsible for consideration and recommendation to EXCO.

7 IMPLEMENTATION

The management of NDLAMBE Municipality are responsible for the implementation of the policy in their own areas.

The management of NDLAMBE Municipality as indicated below are responsible for drafting strategies, sub-policies and standards in support of this policy.

IT or the department responsible: Hardware/software architecture and standards for Internet access, request for Internet access procedures and the processing thereof, Internet Information protection, Security standards and infrastructure Charge-Out Procedures (if applied and implemented).

Any sub-policies/addendums must be derived from Municipalities policies and be in support of NDLAMBE Municipality's overall Internet philosophy. Such Sub-policies/addendums must be approved by Exco, even though these additional documents may seem to conform to the Municipalities policy.

8 ROLE PLAYERS

The major role players in the NDLAMBE Municipality Internet channels are:

- NDLAMBE Municipality IT
- NDLAMBE Municipality **department responsible**

The responsibilities of each role player in the total risk management process of NDLAMBE Municipality's Internet channels shall be:

Ensure that an NDLAMBE Municipality Internet Policy exists.

To review the Internet policy.

To recommend the policy to Exco.

To obtain the approval of Exco on the policy.

To ensure adequate and cost effective management and control structures exist for the proper use of NDLAMBE Municipality's Internet services.

To compile and implement policies and procedures to effectively manage risks regarding the Internet.

To comply with their assigned responsibilities as contained in the Internet Policy.

9 POLICY STATEMENTS

The following constitutes the core of the Internet/Extranet/Intranet policy and will be supported by specific, detailed explanatory standards and/or procedures as defined by policy role players.

- 9.1 The Internet resources provided in the work place at all times remains the property of NDLAMBE Municipality.
- 9.2 The resources so provided are intended to be used specifically for the employee's work and/or work related activities.
- 9.3 Incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with worker productivity, (c) does not pre-empt any business activity and (d) does not exclude the intent of this policy. (See also paragraph 9.2).
- 9.4 NDLAMBE Municipality reserves the right to read any electronic mail message and attachment if it believes the situation warrants it. The employee should have no expectation of privacy in relation to information transmitted and/or stored on an NDLAMBE Municipality provided resource. By signing the Internet/e-mail Application form the employee wavers any right to invoke the provisions of the Interception and Monitoring Prohibition Act 127 of 1992.

9.5 Unacceptable uses of the Internet and Ndlambe Municipality e-mail

- 9.5.1 NDLAMBE Municipality's e-mail and Internet access may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or X-rated. Sending of racially or sexually harassing message/files is also prohibited. No abusive, profane or offensive language is to be transmitted through NDLAMBE Municipality' e-mail or Internet system (including any messaging system such as Winpop, Instant Messenger or any other messenger systems).
- 9.5.2 Electronic media may not be used for any other purpose that is illegal or against NDLAMBE Municipality policy or contrary to NDLAMBE Municipality's best interest. Solicitation of non-NDLAMBE Municipality business or any use of NDLAMBE Municipality e-mail or Internet for personal gain is prohibited. The use of e-mail to participate in political activities, solicit political support or propagate political views is prohibited.(May want to take out the yellow highlighted section?)
- 9.5.3 Copyrighted material belonging to entities other than NDLAMBE Municipality, may not be transmitted by employees on NDLAMBE Municipality's e-mail/Internet system. All employees obtaining access to

other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with written permission of the copyright holder, or as a single copy for reference/back-up purposes only.

9.6 *Acceptable uses of the Internet and NDLAMBE Municipality e-mail:*

- 9.6.1 Every staff member has a responsibility to maintain and enhance NDLAMBE Municipality's public image and, to use e-mail and access to the Internet in a responsible manner (Net etiquette).
- 9.6.2 Internet access is provided for business use only. Internet users have a responsibility to use the Internet appropriately in conducting the municipalities business.
- 9.6.3 Each employee is responsible for the content of all text, audio or images that they place or send over the company's e-mail/Internet system. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else or someone from another company or Municipality. All messages communicated on NDLAMBE Municipality's e-mail/Internet system must contain the employee's name.
- 9.6.4 Any messages or information sent by an employee to another individual outside of the company via an electronic network (e.g. bulletin board, online server or Internet) are statements that reflect on NDLAMBE Municipality.
- 9.6.5 All out-going e-mail will have the NDLAMBE Municipality standard "disclaimer" attached (See Annexure A for an example of a "standard disclaimer")
- 9.6.6 All NDLAMBE Municipality employees are accountable, for the expression of personal or Municipal opinions on the Internet and specifically on news groups.

9.7 *Architecture and Infrastructure:*

- 9.7.1 NDLAMBE Municipality connections to the Internet shall conform to the prevailing Technology Architecture of NDLAMBE Municipality.
- 9.7.2 NDLAMBE Municipality IT, representing NDLAMBE Municipality, shall enter into an agreement with an accredited external Internet Service Provider (ISP), or multiple Internet Service Providers if it is in NDLAMBE Municipality's best interest, for access to the Internet. These agreements shall be the only official NDLAMBE Municipality approved Internet connection. No other NDLAMBE Municipality department may negotiate its own separate Internet access.
- 9.7.3 Only NDLAMBE Municipality IT are allowed to negotiate Web-hosting services. All NDLAMBE Municipality's Internet pages will be hosted at a central Web-hosting server supporting the necessary system redundancy, security, and service level agreements.

9.8 *Adherence*

- 9.8.1 All NDLAMBE Municipality's information and services on the Internet must adhere to the strategy, standards and procedures as described in this policy namely; Internet Design, implementation and presentation standards; Hardware/software standards for Internet access; Request for Internet/Intranet access procedure; Legal guidelines and standards; Internet outsourcing standards; Internet Information Protection security standards; Charge-out procedures; Inter/Intranet Infrastructure Collaborative Web strategy; and Internet/Intranet/Extranet strategies.
- 9.8.2 Failure to comply with the NDLAMBE Municipalities internet/Intranet/Extranet Policy or any of its directives and standards will result in disciplinary action being taken (see Section 9 for possible actions).
- 9.8.3 NDLAMBE Municipality reserves the right to cancel/remove any users Internet access rights and/or application if this can be shown to be in the best interests of NDLAMBE Municipality.
- 9.8.4 NDLAMBE Municipality reserves the right to "block" access to any category or individual Internet site that can be shown as not to be in the best or business interests of NDLAMBE Municipality.
- 9.8.5 All material on a NDLAMBE Municipality Internet site must not violate, plagiarise or infringe upon the right of any third party, including copyright, trademark or proprietary rights.

9.9 Security (see also section 12)

- 9.91 Internet users should at all times adhere to the current Internet security practices within NDLAMBE Municipality when sending confidential or mission critical information across the Internet.
- 9.92 NDLAMBE Municipality reserves the right to monitor any employees Internet/Intranet communications and usage. All messages created, sent, or retrieved over NDLAMBE Municipality's e-mail/Internet are the property of NDLAMBE Municipality and will be considered company information. Employees should not assume electronic communications are totally private and should transmit highly confidential data in other ways. However, to protect employee's privacy, no one will be allowed to access the system to read other mail without prior approval from NDLAMBE Municipality's ITSC. This will provide some assurance that there won't be rampant review of e-mail.
- 9.93 The provision of security is important and all services and information provided on the Internet will comply with the latest NDLAMBE Municipality Internet security standard regarding: authentication, non-repudiation (of origin and receipt) and data integrity and data privacy. The NDLAMBE Municipality Information Technology department must approve all NDLAMBE Municipality Internet application security issues prior to implementation.

9.10 Outsourcing

- 9.10.1 Approval of Internet content development outsourcing will depend on the following:

NDLAMBE Municipality Direct approval for:

- Alignment with NDLAMBE Municipality's Internet strategy;

- Constituent relationship and support functions in compliance with the NDLAMBE Municipality Internet Customer Care policies;
- Compliance to the NDLAMBE Municipality Internet standards and procedures.

- Ensure compliance to NDLAMBE Municipality’s Application Standards for Internet development and Internet web server hosting.

NDLAMBE Municipality Technical Support approval for:

- Type of service to be outsourced and its future integration with NDLAMBE Municipality's Internet technical infrastructure;
- Ensure compliance with NDLAMBE Municipality’s Internet Information Protection and Security standards.

NDLAMBE Municipality Technical Strategy and Architecture approval for:

- Ensuring compliance with NDLAMBE Municipality’s Technical Hardware and Software strategy and architecture.

9.10.1.1 The transferring of ownership and responsibility of NDLAMBE Municipality Internet information and/or services will not be allowed when outsourcing Internet development. All NDLAMBE Municipality Internet information will reside within NDLAMBE Municipality premises to ensure efficient management and control of it. Fragmentation and duplication of NDLAMBE Municipality information and/or services at external outsourced vendors will not be allowed.

10 VIOLATIONS AND PENALTIES

Any employee who abuses the privilege of NDLAMBE Municipality facilitated access to e-mail or the Internet will be subject to disciplinary action, which may result in dismissal. If necessary, NDLAMBE Municipality reserves the right to advise appropriate legal officers of any illegal violations.

The following general guidelines may be used for the purposes of disciplinary action against employees who breach this policy:

11 Offence / Category

Offence	/	1 st Offence	2 nd Offence	3 rd Offence	4 th Offence
---------	---	-------------------------	-------------------------	-------------------------	-------------------------

Category				
Loading illegal software or offensive, disruptive, insulting or immoral material, such as pornographic material, onto a NDLAMBE Municipality owned computer.	Final Written Warning/ Dismissal	Dismissal		
Sending external messages without NDLAMBE Municipality's standard disclaimer attached.	Written Warning	Final Written Warning	Dismissal	
Accessing pornographic, offensive, immoral, insulting, disruptive or discriminatory material.	Final Written Warning/ Dismissal	Dismissal		
Changing the configuration of any Internet server, Server or PC without proper authorization.	Written Warning	Final Written Warning	Dismissal	
Using NDLAMBE Municipality Internet resources for personal gain.	As per the Municipalities disciplinary code on conducting unauthorized private business.			
Excessive browsing on the internet where it is clear that the sites visited are not work related or in any way linked to the services provided by NDLAMBE Municipality.	Written Warning	Final Written Warning	Dismissal	
Browsing on the internet where such browsing leads to deterioration in the employee's performance and quality of work.	Written Warning	Final Written Warning	Dismissal	
Disclosure of Security IDs and passwords to any other person, including non-staff members.	Final Written Warning	Dismissal		
Willfully downloading and/or opening of virus-infected files.	Final Written Warning	Dismissal		
Transmitting of	Final Written			

copyrighted materials without authority of the copyright holder.	Warning / Dismissal	Dismissal		
Disseminating pornographic, offensive, immoral, insulting, disruptive or discriminatory material.	Final Written Warning / Dismissal	Dismissal		
Transmitting or forwarding of chain letters via the e-mail system (including power point slides, Flash files or any other similar formats)	Written Warning	Final Written Warning	Dismissal	
Accessing information available on Internet servers for which you are not authorized.	Final Written Warning	Dismissal		
Sending external messages containing personal opinions and/or statements which may be deemed to be NDLAMBE Municipality's opinion.	Final Written Warning	Dismissal		

12 ELECTRONIC MAIL SECURITY

12.1 Municipal Property:

As a productivity enhancement tool, NDLAMBE MUNICIPALITY encourages the legitimate organisational use of electronic communications. Electronic communications systems, and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of NDLAMBE MUNICIPALITY.

12.2 Authorized Usage:

NDLAMBE MUNICIPALITY electronic communications systems generally must be used only for Municipal related activities. Incidental personal use is permissible so long as:

- (a) It does not consume more than a trivial amount of resources,
- (b) Does not interfere with worker productivity, and
- (c) Does not pre-empt any Municipal business activity.

Users are forbidden from using NDLAMBE MUNICIPALITY electronic communication systems for charitable endeavours, private business activities, or amusement/entertainment purposes.

Employees are reminded that the use of municipal resources, including electronic communications, should never create either the appearance or the reality of inappropriate use. Access to private e-mail accounts is prohibited as it is a source

of security risk. Private internet banking is permissible where individuals have already been granted access to the internet in terms of work requirements, providing the above rules are applied.

12.3 Default Privileges:

Employee privileges on electronic communication systems must be assigned such that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of “least privilege”. Broadcast facilities (such as an “everyone” or “send to all” e-mail) must be used only after the permission of a department manager has been obtained and should be distributed by the relevant mail administrator.

12.4 User Separation:

Personal user-ids and associated passwords must be used to identify and authenticate different users and to isolate the communications of different users. Fax machines that do not have separate mailboxes for different recipients need not support such user separation.

12.5 User Accountability:

Regardless of the circumstances, the policies that apply to id's and passwords in NDLAMBE MUNICIPALITY should also be applied to access of e-mail. Ignoring these exposes the authorized user to responsibility for actions the other party takes with the password. If users need to share computer resident data, they should utilize message forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms.

12.6 User Identity:

Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.

12.7 No Default Protection:

Employees are reminded that NDLAMBE MUNICIPALITY electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communication systems, encryption or similar technologies to protect the data must be employed. Assistance can be obtained from the Information Technology department.

12.8 Respecting Privacy Rights:

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. NDLAMBE MUNICIPALITY is committed to respecting the rights of its employees, including their reasonable expectation of privacy. NDLAMBE MUNICIPALITY also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

12.9 No Guaranteed Message Privacy:

NDLAMBE MUNICIPALITY can however not guarantee that electronic communications will be private. Employees should be aware that electronic communications, depending on the technology, can be forwarded, intercepted, printed, and stored by others. Furthermore, electronic communications can be accessed by others in accordance with this policy.

12.10 Regular Message Monitoring:

It is the policy of NDLAMBE MUNICIPALITY NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that NDLAMBE MUNICIPALITY will and may from time to time examine the content of electronic communications.

12.11 Statistical Data:

Consistent with generally accepted practice, NDLAMBE MUNICIPALITY collects statistical data about electronic communications. Using such information, technical support personnel can monitor the use of electronic communications to ensure the ongoing availability and reliability of these systems.

12.12 Incidental Disclosure:

It may be necessary for technical support personnel to review the content of an individual employee's communications during the course of problem resolution. Technical support personnel may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels.

12.13 Contents of Messages:

Workers must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others. Such remarks -- even when made in jest -- may create legal problems such as trade libel and defamation of character. Special caution is warranted because back-up and archival copies of electronic mail may actually be more permanent and more readily accessed than traditional paper communications.

12.14 Message Forwarding:

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. NDLAMBE MUNICIPALITY sensitive information must not be forwarded to any party outside NDLAMBE MUNICIPALITY without the prior approval of a local department manager. Blanket forwarding of messages to parties outside NDLAMBE MUNICIPALITY is prohibited unless the prior permission of the Information Security Manager has been obtained.

12.15 Handling Information About Security:

Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the IT department. Users are prohibited from utilizing NDLAMBE MUNICIPALITY systems to forward such information to other users, whether the other users are internal or external to NDLAMBE MUNICIPALITY.

12.16 Public Representations:

No media advertisement, Internet home page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about NDLAMBE MUNICIPALITY may be issued unless it has first gone through the appropriate approval channels.

12.17 User Back-Up:

If an electronic mail message contains information relevant to the completion of a transaction, contains potentially important reference information, or has value as evidence of a NDLAMBE MUNICIPALITY management decision, it should be retained for future reference. Most electronic mail messages will not fall into these categories, and accordingly can be erased after receipt. Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail systems are not intended for the archival storage of important information. Important stored electronic mail

messages can be periodically expunged by systems administrators, mistakenly erased by users, and otherwise lost when system problems occur.

12.18 Archival Storage:

All official NDLAMBE MUNICIPALITY electronic mail messages, including those containing a formal management approval, authorization, delegation, or handing over of responsibility, or similar transaction, must be archived.

12.19 Purging Electronic Messages:

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After a certain period -- generally six months -- electronic messages stored on multi-user systems will be automatically deleted by systems administration staff. Not only will this increase scarce storage space, it will also simplify records management and related activities.

12.20 Harassing or Offensive Materials:

NDLAMBE MUNICIPALITY computer and communications systems are not intended to be used for, and must not be used for the exercise of the workers' right to free speech. Sexual, ethnic, and racial harassment --including unwanted telephone calls, electronic mail, and internal mail -- is strictly prohibited and is cause for disciplinary action. Workers are encouraged to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications. If the originator does not promptly stop sending offensive messages, workers must report the communications to their manager and the Human Resources Department. NDLAMBE MUNICIPALITY retains the right to remove from its information systems any material it views as offensive or potentially illegal.

12.21 Access to Internet E-mail:

Internet based electronic mail may only be accessed via the internet email servers provided by NDLAMBE MUNICIPALITY when the target computer is linked to the NDLAMBE MUNICIPALITY network. Users are not allowed to e.g. dial out to service providers in order to access e-mail. Downloading of private e-mail from external mail accounts (e.g. Hotmail, Yahoo, MSN, etc) is prohibited.

12.22 Virus Scan of E-mail:

All inbound and outbound electronic mail must be scanned for viruses before delivery. The scanning should include attachments zipped or otherwise. The exception would be encrypted email. Specific policies relating to encrypted mail apply in this case.

13 STANDARD E-MAIL DISCLAIMER

An example of a standard e-mail disclaimer is presented below. The disclaimer is presented at footer of the e-mail and is normally created as a default text that is automatically applied when a new e-mail is created. This is normally setup as a stationary element in the e-mail client configuration. It is the responsibility of the IT department to ensure that the disclaimer is automatically configured on the user's computer or e-mail client.

The purpose of the disclaimer is to protect the municipality from litigation arising from the accidental disclosure of information to an unintended third party, from damage to a third parties computer system resulting from a computer virus or any other harmful program hidden in or embedded into an e-mail or attachment to an e-mail.

The e-mail footer, in addition to the disclaimer, should contain the organisation from which the e-mail is being transmitted, the E-mailer's name and contact information. This is required so that any individual receiving an e-mail in error can notify the originator and destroy the e-mail without any copies of the mail being retained.

Example of a Standard E-mail Disclaimer

"This message may contain information which is confidential, private or privileged in nature and subject to legal privilege. If you are not the intended recipient, you may not peruse, use, disseminate, distribute or copy this message or file which is attached to this message. If you have received this message in error, please notify the sender immediately by e-mail, facsimile or telephone and thereafter return and/or destroy the original message.

Please note that the recipient must scan this e-mail and any attached files for viruses and the like. NDLAMBE Municipality accepts no liability of whatever nature for any loss, liability, damage or expense resulting directly or indirectly from the access of any files which are attached to this message."