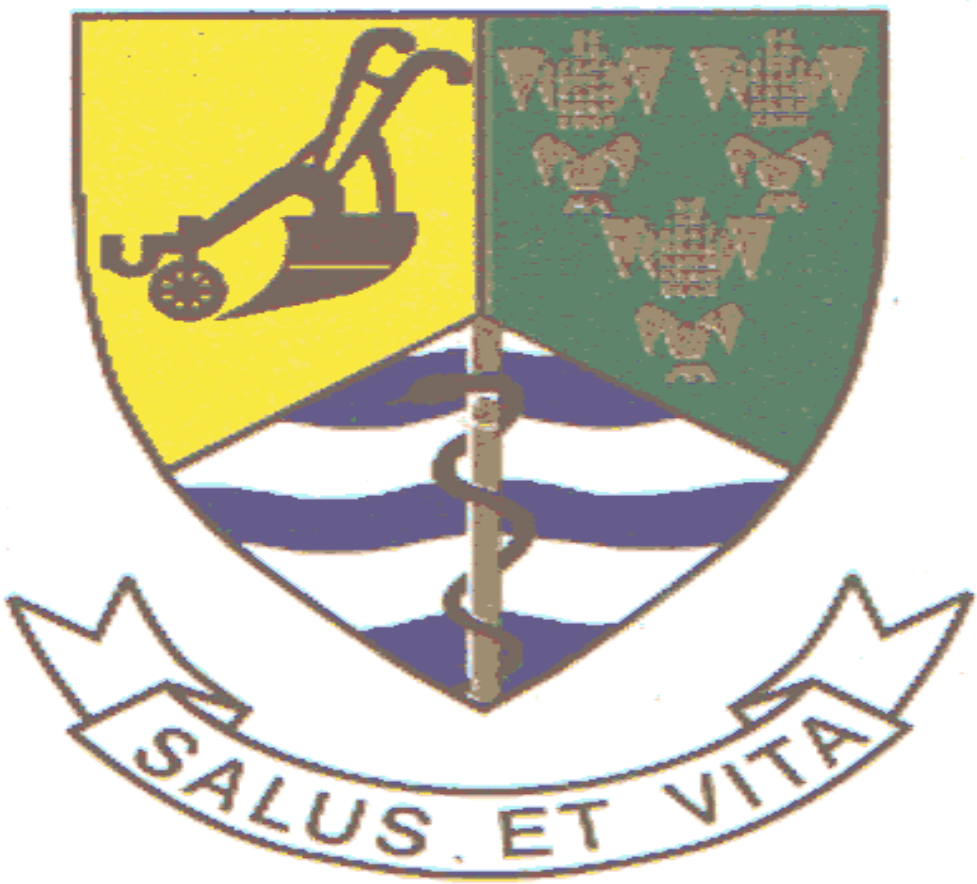
# ELECTRONIC MAIL AND INTERNET USAGE POLICY




Date: 21/03/2009

**Approvals**

Head of Department

Signature…… Date……..

Municipal Manager

Signature…….. Date…….....

Divisional Manager: Information Management

Signature…….. Date……..

TABLE OF CONTENTS

## 1. Introduction

Bela-Bela Municipality provides e-mail facilities to all employees, contractors and service providers who utilize its network and/or network resources to enhance business operations, E-mail can help the Municipality improve the way it conducts business by providing a quick and cost-effective means to create, transmit, and respond to messages and documents electronically and to improve the sharing of information in an effort to accelerate service delivery to the public. The Municipality recognizes that principles of freedom of speech, confidentiality and integrity of information have implications on the use of email facilities such that the
Municipality will in future implement e-mail content filtering systems to ensure that the use of e-mail facilities is in line with the municipal requirements and objectives. This Policy reflects these firmly-held principles within the context of the Municipality'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

- Protect the integrity and public image of Bela-Bela Municipality
- Help boost productivity and prevent misuse of email facilities and network resources by clearly defining rules and restrictions for personal use.
- Ensure that Email users are notified about the applicability of laws, regulations, standards, guidelines and best practices
- Prevent monopolizing of resources
- Assure that disruptions to Municipality's email facilities are minimized
- 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 the Municipality's email facilities or any emails sent via Bela-Bela Municipality's internet facilities. It applies to all municipal officials, as well as SITA, National and Provincial Local Government Departments, State Owned Entities (SOE), the Private Sector and third parties that might be operating on behalf of Bela-Bela Municipality. This policy only applies to the usage of Internet and electronic mail in its electronic form and it does not address printed copies of electronic mail.

## 4. References, Related Legislation and Regulations

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

SABS/ISO 17799
Information Security Forum (The standard of good practice for Information Security)
Minimum Information Security Standards
Copyright Act
Protection of Information act
Promotion of Access to Information Act of 2000
Public Service Act
National Strategic Intelligence Act
Interception and Monitoring bill
Regulation of Interception of Communications and Provisions of Communication-Related Information Act
COBIT Audit framework
Electronic Communications and Transactions Act
National Archives of SA Act 43 of 1996
International Standard for Risk Assessment
Limpopo Provincial Information Security Policy

## 5. Cautions

Bela-Bela Municipality 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, Bela-Bela Municipality can assure neither the privacy of an individual user's use of Municipal electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

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

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 E-mail / Exchange Administrator to verify the authenticity of the message. Furthermore every email attachment should be scanned for viruses before being opened.

E-mail users are expected to use Bela-Bela Municipality Email facilities responsibly, that is, comply with laws of RSA, other policies and procedures put in place by Bela-Bela Municipality, and with normal standards of professional and personal courtesy and conduct. Access to Bela-Bela Municipality E-mail facilities, when provided, is a privilege that may be wholly or partially restricted by the municipality 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 Bela-Bela Municipality procedures or, in the absence of such procedures, to the approval of the Departmental Head.

## 6. Email Security Policy

Electronic Mail (Email) functions much like ordinary mail. The sender writes an electronic letter and may add, if needed, enclosures such as text documents, graphics or spreadsheets. The sender then 'posts' the message by adding the recipient's Email address, often selected from an electronic address book. These Email addresses may be people, departments or functions and include names and some indication of location.

Email uses resources that can be distributed over several data networks. The user's conduct contributes to whether or not the availability and confidentiality of the system is ensured.

### 6.1 Risks of E-mail

Since e-mail includes both the transmission and handling of sometimes-sensitive information, care must be taken to protect the message from unauthorized access.

Threats can include the ability of individuals to change and copy information, or to distribute information to unauthorized parties. Users can also act anonymously, or with a fake identity, and spread information under assumed names.
The use of e-mail is therefore open to a number of commercial risks, including:

- Distribution of messages through error or negligence
- Unauthorized use, processing or distribution of messages
- Distortion, interruption or unwanted disclosure of messages
- Unauthorized disclosure of confidential, proprietary or trade secret information

### 6.2. E-Mail Naming Standards

The following naming standards have been agreed to and will apply for all BBM e-mail users:

- The surname and first initial of the user will be used as the e-mail id
- When defining a new username or e-mail id, if such name already exists, the second initial will be utilized.
- No nicknames will be used as network or e-mail identities.

### 6.3. Size Limits of Mailboxes, and Attachments

All Email users have uniform quota limits set on their individual mailbox. Users close to their limit will be notified and the mailbox will be closed once this limit is exceeded. ITO 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 ITO for advice on mailbox management.

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all E-mail 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.

The following limits will apply and adhered to by all BBM e-mail users:

- A size limit of 10 MB for mailboxes.
- A size limit of 20MB for Sending and receiving mail, inclusive of original message plus attachments.

### 6.3. E-Mail Policy Statements

- Private use is permitted but this is subject to strict control. Abuse of this privilege may be regarded as misconduct.
- From time to time the use of the Email system may be audited.
- The Municipality reserves the right to inspect the e-mail at any time without notice.
- Through using Email you will have been deemed to have read, understood and agreed to the policies relating to e-mail systems contained within these documents.
- Do not as matter of course forward confidential, trade secret or proprietary information to third parties. Delete any unnecessary e-mail you receive from the Email system after having been read.
- Do not send all messages as confidential as this negates the purpose and adds unnecessary overheads to the e-mail systems.
- Check any e-mail enclosures for viruses, BEFORE opening, particularly if documents containing executable programs are sent. If users open a message and are prompted to “Enable or Disable macros” users should select “Disable” and scan for viruses. If any Viruses are found then notify the Information Technology Office.
- If users get an attachment via Email, which is unsolicited, or of unknown origin, detach it and scan the file using the installed anti-virus software. Alternatively delete it.
- Avoid unnecessarily large distribution lists.
- Check your mailbox regularly for received mail.

- Ensure that the content of the message cannot be misinterpreted and that there is nothing unlawful about the transmission or content of the message.

***NB: Always click send and receive every time once opening your Outlook***

- From time to time, certain disclaimers may be required for messages requiring confidentiality, legal privilege etc. Request assistance from the Municipality's legal Officer.
- It is prohibited to forward or transmit: Offensive, defamatory, discriminatory or harassing material, Sexually explicit or other offensive images, Unlicensed copyright material, non- business related video and image files, confidential, proprietary or trade secret information outside without authorization, advertisements and chain letters.
- Do not send or forward E-mail notices concerning virus or harmful code warnings to other employees.
- Avoid sending messages with large attachments. Large attachments can be compressed (with a utility such as WinZip).
- Do not send a large number of Email messages to a single address as it may disable the destination mailbox.
- Do not "broadcast" Email messages unnecessarily.

**When using electronic mail to communicate with people on the Internet:**

i. Do not automatically forward internal mail to an Internet site.

ii. Do not use auto-reply functions to respond to your Internet mail.

iii. When using the auto-reply functions such as Out of Office message option for normal municipality's internal mail, be sure to select the option that excludes sending the notices to Internet users.

iv. Users shall not use an electronic mail account assigned to another individual to

v. either send or receive messages.

vi. Users should regularly move important information from electronic mail message files to word processing documents, databases, and other files, as Email messages may be erased periodically, either accidentally or as part of normal archiving and file maintenance functions.

vii. If users receive unwanted and unsolicited email (also known as SPAM), they shall refrain from responding directly to the sender. Instead, they should contact Information Technology Division.

viii. E-mail is a vital communications tool for the municipality. Users should therefore access their E-mail INBOX as often as possible. Unopened Email older than one calendar month will be deleted from the server.

ix. It is the responsibility of individual users to manage their own E-mail once they have downloaded it. It is suggested that unwanted E-mails are regularly deleted and important E-mails are moved to appropriate folders (e.g. Nancy PST). Contact the Information Division should further information regarding the management of Email be required.

## 7. Internet Security Policy

The Municipality's information, computing assets, and corporate image on the Internet are critical to our success, and as a result, must be protected from loss, modification or destruction.

The Internet is used to connect with our customers, suppliers and other organizations.

It is important to remember the following points:

- The Internet is used by millions of people worldwide.
- Unprotected information sent across the Internet may well be read by any number of unknown people.

### 7.1. Risks of the Internet

On the Web, one of the real dangers is a possible loss of company privacy or leakage of information about the municipality's activities. The following issues relate to users privacy when surfing the web:

When users visit a web site, the site they are visiting can identify where their Internet connection originates. For example, if users use the Web from work, activities can be identified as coming from the municipality**.** Web sites can log all of users' activity including any personal data they provide. The web site owner can associate users with this data on future visits. Some web sites do not respect data privacy laws and may make the information collected from you available to other organizations.

## 7.2. Virus

Viruses are designed at best to cause some discomfort and at worst to cause the alteration and loss of data on a computer. Viruses pose a tremendous threat and can be introduced in a number of ways, particularly from files and programs downloaded from internet sources and via email attachments. It is therefore imperative that all computers in use have approved anti-virus software loaded and activated, and that this software is regularly updated. Contact the Information Technology Division if you are in any doubt about either a message or file content or for more information about Anti-Virus software.

## 7.3. Internet Security Policy Statement

- Automatic access to the Internet is not a right, and access can be revoked if it is found that misuse of the facility is occurring.

- Whenever an employee posts a message to an Internet discussion group, an electronic bulletin board, or another public information system, this message shall be accompanied by words clearly indicating that the comments do not necessarily represent the position of the municipality.

- Unless expressly authorized by the Municipal Manager, when using Municipality information and/or systems, all employees are forbidden from participating in Internet discussion groups, chat rooms, or other public electronic forums except for work related purpose.

- Users shall not advertise, promote, present, or otherwise make statements about municipality products and services in Internet forums such as mailing lists, news groups, or chat sessions without the prior approval of the Municipal Manager.

- Although the Internet is an informal communication environment, the laws for copyrights, patents, trademarks etc. apply. Employees using Municipality internet or communication systems shall:
- Resend material only after obtaining permission from the source.
- Quote material from other sources only if these other sources are identified.

- Reveal internal municipality's information on the Internet only if the information has been officially approved for public release by the municipality's Communication section.

- When using the municipality's information systems, or when conducting municipality's business, employees shall not deliberately conceal or misrepresent their identity.
- Information Technology Division may prevent users from connecting with certain non-business web sites. The ability to connect with a specific web site does not in itself imply that employees are permitted to visit that site.

- No user or independent contractor to the municipality may use the available Internet or E-mail services provided by municipality to access newsgroups, Internet web sites and FTP sites for unauthorized and/or unacceptable purposes such as, but not limited to the viewing and/or downloading of pornographic or obscene material of any nature;

- All software and files down-loaded from internet sources via the Internet (or any other public network) shall be screened with approved virus detection software before being run or examined via another program such as a word processing package.

- All users wishing to establish a connection with the municipality's computers via the Internet shall authenticate themselves at a firewall before gaining access to the municipality's internal network. Contact the Information Technology Division for further information.

- Non-municipality's computers are prohibited from connection to the municipality's networks without specific written permission from the Head of Department.

- Dial out or connections to any non-municipality systems or networks while simultaneously connected to the internal network are prohibited.

- Do not run security-testing tools/programs against any Internet system or server.

- Dial up connections e.g. whilst traveling or from home based systems and laptop computers which are also utilized for municipal business must only be made via authorized dial up

procedures which employ the use of firewalls and configured by Information Technology Division.

## 8. Passwords Policy

- A computer access password is the primary key to computer security. The importance of password maintenance and security cannot be over emphasized.

- All employees and uses of the municipality's computer facilities are solely responsible for the integrity and secrecy surrounding passwords allocated for their usage.

- The password uniquely identifies employees and users, and allows access to the municipality's information and computer services. For your own protection, and for the protection of the municipality's resources, you must keep your password secret and not share it with anyone else.

- Contact the Information Technology Division if any further password information is required, or if there is any uncertainty surrounding the usage, applicability, installation or issuing of passwords.

- Users create their own password on their computers and IT Office have the right to reset, over-write once the user has forgotten or request it to be changed.

### 8.1. Password Policy Statements

- All user-chosen passwords for computers and networks shall be difficult to guess.

- Construct fixed passwords by combining a set of a minimum seven alphanumeric characters

- Do not construct passwords, which are identical or substantially similar to passwords previously used

- Passwords shall not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them.

- All vendor-supplied default passwords shall be changed before any computer or communications system is used.

- All passwords shall be changed immediately if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.

- Regardless of the circumstances, passwords shall never be shared or revealed to anyone else by the authorized user.

- Users are responsible for all activity performed with their personal user-Ids, Shall not allow the user-IDs to be used by anyone else and shall not perform any activity with other users' Ids.

- Employee and user generated passwords should in general have the following characteristics:
    - Be at least 8 characters in length
    - Contain at least one alphabetic and one non-alphabetic character
    - Not contain the user id as part of the password.
- All users will be forced to change passwords every 30 days. Contact the Information Technology Division if any further password information on changing or issuing of passwords.
- Normal windows screen savers should be activated after 10 minutes of inactivity as a maximum, and should be password controlled.
- Passwords will automatically logout after 3 attempts.
- Certain systems i.e. Financial Management System has specific password requirements over and above those shown above. These systems will prompt the user for the correct information. If in any doubt, contact the Information Technology Division for further information.

- Should users forget their password, they must contact the Information Technology Division for assistance.

## 8.2. External E-mail 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 e-mail accounts are outside the control of IT Officers or
Bela-Bela Municipality 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 Bela-Bela Municipality's computer network. There are also confidentiality concerns with these applications and as a result Instant Messaging Applications other than those authorized by Bela-Bela Municipality are prohibited.

## 8.3. Prevention of Malicious Software

E-mails are subjected to huge amounts of malicious software including viruses, computer worms and spyware. As a result, Bela-Bela Municipality with assistance from SITA and DPLGH 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:
By default all virus infected mails will be blocked
All attachments that cannot be scanned for viruses will also be blocked
Typical virus hoaxes will be blocked
All executable files or documents with embedded executables will be blocked. (Please refer to Annexure C for a list of prohibited executable files)
All unknown/unrecognizable attachments will be blocked

## 8.4. Communication of Official Information

E-mail users are expected to use Bela-Bela Municipality email facilities in accordance to municipal 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 division 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.

## 9. Limitation of Privacy

E-mail 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 Bela-Bela Municipality's Email facilities.

While Bela-Bela Municipality 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 Bela-Bela Municipality 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 Office or via email reply to the e-mail message indicating policy breach. Authorized Bela-Bela Municipality's personnel will only upon this request access the blocked e-mail as to carry out further investigation. Thus by sending a message release request, the Email user consents Bela-Bela Municipality to access only the email message in question. Furthermore responsible official will not inspect the specific content of blocked email messages unless if the concerned contains a virus. For purposes of ensuring reliable E-mail facilities and diagnosing network problems Information Manager may access the e-mail history logs. These logs do not reveal e-mail contents but only the headers.

## 10. Discriminatory, harassing and/or offensive language

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

## 11. Monitoring and Reporting

It must be understood that Bela-Bela Municipality 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, Divisional Manager: Information Management reserves the right to monitor email traffic from time to time for statistics, operation efficiency and reporting. This will ensure that Divisional Manager: Information Management can predict email trends so as to proactively plan for future growth, continuously improve Email security and ensure compliance.

## 12. Access to another employee's e-mail

By default no employee except authorized Divisional Manager: Information Management 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 Divisional Manager: Information Management. Divisional Manager: Information Management will not actively monitor employee mailboxes but it may be necessary for authorized him/her to view the contents of employees' electronic communications and Email activity or history in the course of problem resolution, system maintenance and operational duties. 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.

### 12.1. 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 e-mail user leaves his or her employment at Bela-Bela Municipality or his or her services are terminated, Divisional Manager: Information Management 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 e-mails until he or she can notify contacts about

the new e-mail address. These e-mails will be automatically forwarded for a period of one month. To prevent intentional and unintentional information disclosures, all official's e-mails will be exempt from this automatic forwarding.

### 12.2. E-mail 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.

### 12.3. Dead, chain letters and Hoax and Spam e-mails

Users must not use Bela-Bela Municipality's e-mail 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.

### 12.4. Prohibited Use

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

Distributing chain letters, junk mail and/or hoax email messages
Sending, receiving and storing of pornography and profanity
Sending, receiving and storing of audio and video files
Sending of emails to distribution lists to which you have not been granted the authorization
Sending of classified departmental information
Sending of e-mails of racial, hate, discrimination or sexist nature
Sending of unsolicited personal and commercial advertisements or promotions to other staff members or external email recipients
Sending of other people's confidential and personal information
Sending of data that violates copyright laws
Capturing and viewing of e-mails except when required for authorized IT Officer to diagnose and correct delivery problems as well as investigate policy breaches.
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.
Use of electronic mail in any manner prohibited by national and international laws and regulations
"Email Spoofing" i.e. constructing emails so it appears to be from someone else.

"Snooping" i.e. obtaining access to other people's emails for the purpose of satisfying curiosity
Attempting unauthorized access to electronic emails or attempting to breach security systems of any e-mail system or "eavesdropping" i.e. attempting to intercept any electronic mail transactions without proper authorization.

## 13. Disclaimer

All e-mail messages sent from Bela-Bela Municipality's email facilities will automatically be stamped with the following disclaimer:

"This e-mail and any attachments thereto may contain confidential and proprietary information and is intended for the recipient only. If you are not the intended recipient, kindly delete the entire communication and notify the sender thereof immediately as the information contained in this communication is protected by law and may be privileged. You are further reminded that copying, distribution or disclosure of the contents of this email may be unlawful and result in legal action against you, in the case of you not being the intended recipient. As information sent by e-mail is corruptible, Bela-Bela Municipality does not accept responsibility for such corruption, destruction, loss or interference of whatsoever kind and howsoever caused"

## 14. Authorization Procedures

A user will be granted access to e-mail and internet 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 Divisional Manager: Information Management or the HR Officer. The signed undertaking will be filled in the staff file of the employee. Divisional Manager: Information Management/HR Office 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.

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. E-mail resources will not be available to any user who does not agree to abide by and be legally bound by this Policy.

## E-mail User's Responsibilities

All e-mail users are responsible, accountable and liable for all their activities while using the Municipal e-mail facilities. As such the e-mail user has the following responsibilities:
Ensure that their usernames and passwords are kept secure and not shared
Fully comply with all aspects of this policy
Immediately alert Div. Manager: Information Management/IT Office about any misuse and non-compliance.
Duty not to waste computer/network resources
Continuously protect the integrity and public image of Bela-Bela Municipality

## Information Technology Responsibilities

Implement technical measures to ensure adequate Confidentiality, Availability and Integrity of Bela-Bela Municipality's e-mail facilities
Monitor and enforce policy compliance
Follow appropriate channels to resolve policy breaches and incidents
Educate e-mails users whenever possible about Email security best practices and this Electronic Mail Acceptable Use Policy.

## Security Implications

The use of electronic mail services exposes BBM and users to network and, in particular, Internet related risks. Even with the extensive effort that has been made by the BBM to minimize known risks, there is no known way to protect the Municipality from all related risks. E-mail and network security is a joint responsibility of SITA, Outsourced Financial Service Provider, DPLG, DLGH, ITO and e-mail users. Transmission of electronic mail to locations outside of the Municipality's local area network may require the use of the Internet for transport. Since the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls. Confidential and sensitive information must not be included in e-mail communications unless proper, formalized security precautions have been established. It is the responsibility of the ITO to protect confidential and sensitive information where intentional,

inappropriate, or accidental disclosure of the information might expose the Municipality or an individual to loss or harm.
Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of their e-mail account by unauthorized individuals. Passwords should be changed with regular frequency or in accordance with the BBM's policy regarding the frequency of changing passwords. Obvious passwords should be avoided. When users are away from their desks, precautions should be taken to protect their accounts (preferably shutting down the PC).

## 16. Consequences of Non-Compliance

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

## 17. ANNEXURE A: DECLARATION FORM

**INTERNET & E-MAIL FORM**
SEND THIS FORM TO THE IT OFFICE

**Please enter your personal details:**

| First Name | Surname | Employee No |
|---|---|---|
| ID No | User ID/Profile | E-Mail |
| Phone No | Fax No | Building |
| Department | Division | Office No |

☐ **APPLY E-MAIL INDIVIDUAL ACCOUNT**

☐ **APPLY INTERNET USAGE ACCOUNT**

**DECLARATION**

I understand and will abide by the Municipality's **Internet and Electronic Mail Use Policy** and acknowledge and understand that any violation of this policy will be un-procedural, constitutes an act of misconduct and possibly an offence. I further understand that should I commit any violation, further disciplinary actions may be taken against me.

User signature: _____ Date: _____/_____/_____

Divisional Head: _____ Date: _____/_____/_____

## 18. ANNEXURE B – INTERNET AND ELECTRONIC MAIL USE AGGREEMENT

**USER CONSENT AND ACCEPTANCE**

I,.....

1.1 acknowledge that I have received, read and understand the **BBM** Internet and Electronic Mail Acceptable Usage Policy and accept the principles set out in the policy as binding on me;

1.2 agree that the Municipality may from time to time monitor, access and view all communications created, stored, accessed, viewed, received and/or sent by me using the BBM IT system and that I have no guarantee or expectation to privacy in using the Municipal IT system in accordance with the terms and conditions of this policy;

1.3 Understand and acknowledge that a violation of this policy may result in disciplinary action in accordance with the Municipality's disciplinary procedures, including possible dismissal, as well as civil and criminal liability.

**Signed at**..... **on** ..... **2009**

**NAME:** ..... **SIGNATURE:** .....

**WITNESS (User's Manager/Supervisor)**

Initials & Surname: Date:

..... .....

## 19. ANNEXURE C - Email Content Filtering

**The following file extensions or attachments will be configured on the content Filtering device/software and by default will be blocked,**

- Exe, pif, com, bat, cmd, reg, sys, ini, cpp
- All movie and music types e.g. Mp3, wav avi, mov, mpg, ogm, Real Audio, windows media player streaming audio, flash
- All files with pornographic material
- Pornographic keywords
- Attachments with pornographic url's
- E-mail exceeding 1Mb in size
- All spam email

## Annexure D – Abbreviations and Definitions

| | |
|---|---|
| Computer virus | A computer program or script that interferes with, or damages the normal operation of a computer or any installed software. Virus programs are designed to infect other computers by hiding within e-mails or executable programs. |
| Copyright | Copyright is designed primarily to protect an artist, publisher, or other owner against any unauthorized copying of his works, by reproducing the work in any material form, publishing it, performing it in public, filming it, broadcasting it, causing it to be distributed to subscribers, or making any adaptation of the work. A copyright supplies a copyright holder with a kind of monopoly over the created material, which assures him of both control over its use and the pecuniary benefits derived from it. |
| Municipality | Bela-Bela Local Municipality |
| Prescripts | Regulations, instructions and directions. |
| Removable storage device | A removable disk on which data may be stored. Usually refers to the 3½-inch diskette. For the purpose of this policy this term includes any removable storage device fitted to a personal computer. |
| Personnel | includes employees/staff/officials employed permanently and temporarily as well as supplied by labour brokers or service-providers |
| Personal Computer | Computer Equipment being a Desktop or Laptop/Notebook assigned by **BBM** to personnel for business activities and official use. |
| CASCADING | Cascading is the term often given to the movement of PCs within an organisation |
| Download | Acquiring (getting) a file /data from internet |
| FTP | File Transfer Protocol, used for transferring data/files on the internet |
| Hyperlink | Automatic link to a URL |
| Personal Account | An account created on the computer for individual User for official usage |
| URL | Uniform Resource Locator, the address of a specific website |
| User | Authorised individual, making use of the Municipality IT Infrastructure |

| | |
|---|---|
| BBM | Bela-Bela Local Municipality |
| DPLG | Department of Provincial and Local Government |
| DLGH | Department of Local Government and Housing of Limpopo |
| SITA | State Information Technology Agency |
| ITO | Information Technology Office, managed by the I.C.T Offiers. |
| IP | Internet Protocol |
| PC | Personal Computer |
| ISP | Internet Service Provider |
| CD | Compact Disk |
| GIS | Geographical Information Systems |
| IARF | Information Asset Release Form |
| WWW | World Wide Web |