



## **E-Mail and Internet Policy**

**Effective Date: 10 June 2020**

Document Classification:

**Confidential**

© GEPF 2020

### Table of Contents

1. Document Version.....	3
2. Business Areas Impacted By This Policy.....	3
3. Regulatory Framework .....	3
4. Glossary of Terminology .....	4
5. Policy Objective.....	5
6. Purpose .....	6
7. Scope of Application.....	7
8. Management right to access information .....	7
9. Allocation of email address and internet access.....	7
10. Acceptable use of e-mail and internet.....	7
11. Unacceptable use of e-mail and internet.....	8
12. Personal use of e-mail & internet facilities.....	10
13. General communications .....	11
14. Monitoring e-mail use and internet access.....	11
15. Virus protection .....	12
16. Functional responsibility .....	12
17. Managements' accountability for e-mails used by their personnel .....	12
18. Queries and clarification of policy.....	12
19. Non-compliance and corrective action.....	13
20. Policy review .....	13
21. Approval .....	13
22. Email Guidelines.....	14

### 1. Document Version

Version	Revision Date	Prepared by	Business Unit	Status
V1.0	19 January 2012	Gordon Oyomno	Manager: GPAA ICT	Draft
V2.0	3 April 2012	Joelene Moodley	Corporate Services	Draft
V3	7 August 2012	Siyanda Dyeshana	Manager: Resources	Draft
V4.0	10 May 2017	Musa Mabesa	Finance Manager	Draft
V5.0	12 December 2018	Paul Masipa	Manager: ICT	Final
V6.0	12 February 2020	Paul Masipa	Manager: ICT	Final

### 2. Business Areas Impacted By This Policy

Name Business Unit/Area	Context and Relevance
All users who act on behalf of the GEPP or are in its employment.	To provide guidance concerning management of the use of email and internet access to mitigate the impact of inappropriate usage.

### 3. Regulatory Framework

Statute / Policy/ Regulation	Applicability
Protection of Information Act (84 of 1982)	To provide for the protection from disclosure of certain information; and to provide for matters connected therewith
Electronic Communication and Transmissions Act (ECT) (25 of 2002)	The ECT prescribes the measures taken to secure information, using secure equipment.
GEPP Information Security Policy	The purpose of this policy is to ensure a secure GEPP IT environment. .
Minimum Information Security Standards (MISS)	A minimum information security standard policy approved by Cabinet on 04 December 1996.
ISO / IEC 2700:2005 standard	The ISO 2700:2005 is a set of International standards that concentrates on the establishment of information security through the implementation of suitable set of controls, including policies, process, procedures, structures and functions.
Protection of Personal Information Act, 2013 (Act No. 4 of 2013) (POPIA)	Promotes the protection of personal information by public and private bodies

Statute / Policy/ Regulation	Applicability
<b>Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002</b>	Regulates the interception of communications and associated processes such as applications for and authorisation of interception of communications.

#### 4. Glossary of Terminology

Abbreviation/Terminology	Description
<b>Software</b>	Software owned by, or licensed to the GEPF that enables and facilitates the use of computers/hardware/infrastructure.
<b>Sensitive</b>	Information whose access shall be guarded due to proprietary. Ethical or privacy considerations. This classification applies even though there may not be a civil statute requiring this protection.
<b>Virus</b>	A computer program that interferes with, or damages the normal operation of the computer or software. Virus programs are designed to infect other computers by hiding within e-mails or runnable programs.
<b>Copyright</b>	Copyright is designed primarily to protect an artist, publisher, or other owner against any unauthorized copying of his works. The protection relates to 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 financial benefits derived from it.
<b>Electronic mail /E-mail</b>	Messages transmitted and received by computers through a network. An electronic-mail, or E-mail, system allows computer users on a network to send text, graphics, and sometimes sounds and animated images to other users
<b>Spam</b>	Copies of the same message sent to large numbers of newsgroups or users on the Internet. People spam the Internet to advertise products as well as to broadcast some political or social commentary.
<b>Hacking</b>	Unauthorized attempts to bypass the security mechanisms of an information system or network.
<b>Internet Access</b>	To be connected to the Internet in order to search/source information.
<b>Internet Browser</b>	A software application for retrieving and presenting information resources on the World Wide Web.
<b>Network</b>	Group of computers that are connected to each other for the purpose of communication.

Abbreviation/Terminology	Description
<b>Web Browser</b>	A software application for retrieving, presenting, and traversing information resources on the World Wide Web.
<b>Website</b>	Collection of related web pages, images, videos or other digital assets that are addressed with a common domain name in an Internet based network.
<b>WWW (World Wide Web)</b>	A way of accessing information over the Internet. It is an information-sharing model that is built on top of the Internet.
<b>COBIT</b>	Control Objectives for Information Technology
<b>GEPF</b>	Government Employees Pensions Funds
<b>Trustees</b>	Trustees refers to Trustees as well as Substitute Trustees
<b>User</b>	Anyone with authorised access to the GEPF business information systems, including permanent and temporary employees, Trustees or third-party personnel such as temporaries, contractors, consultants, and other parties with valid GEPF access accounts

### 5. Policy Objective

Electronic mail and internet is one of the most important and most effective communication mechanisms in use within the GEPF and users place a high measure of reliance on the effective use and operation of this technology.

This policy aims to define, implement and manage controls to manage the acceptable use of organisation internet and email to protect the GEPF from information assets from the risk of unauthorised access, damage, disruption and other threats, be it internal or external, deliberate or accidental.

#### Internet Usage

Internet usage by users shall be for GEPF business and support purposes only.

Internet use allows for the possibility of security breaches of confidential GEPF information. Internet use also creates the possibility of contamination to GEPF systems via viruses or malicious software . Malicious software allows unauthorized people potential access to GEPF passwords and other confidential information.

#### Email Usage

Email shall be used for GEPF business and support purposes only. Confidential information shall not be shared outside of GEPF without authorization.

Some of the risks attached to the use of email and internet are:

- Users of the e-mail and internet facility may unintentionally subject the GEPF to legal liability, either through defamation, breach of copyright or by entering into a contract.
- Personal or improper use of e-mail and unauthorised results in lost productivity and unnecessary facility upgrades.

### 6. Purpose

The purpose of this policy is to provide guidance with regards to:-

- Management of email and internet usage to mitigate the impact caused by inappropriate usage;
- Setting of clear guidelines for acceptable and considerate use of electronic mail and internet.

An Internet and E-mail policy dictates what is deemed appropriate, applicable e-mail usage and internet browsing behavior in the workplace. This policy typically enforces restrictions for users when browsing the internet and restricts e-mail outflow and inflows of non-work related tasks as well as stipulating what sites they are allowed to browse. Having an internet and e-mail policy, which can also be referred to as an acceptable use policy (AUP), ensures that user are following directives that serve to safeguard their work environment and the IT network infrastructure within GEPF.

### 7. Scope of Application

This policy applies to all GEPF users and agents with a GEPF-owned or personally owned computer or workstation used to connect to the GEPF network.

### 8. Management right to access information

The GEPF respects the individual privacy of users. However, user privacy does not extend to the employee's work-related conduct or to the use of GEPF-provided equipment or supplies. Users shall be aware that the following guidelines might affect their privacy in the workplace.

The electronic mail system has been implemented by the GEPF to facilitate business communications. Although each user has an individual password to access this system, it belongs to the GEPF and the contents of e-mail communications are accessible at all times to GEPF management and Corporate Services authorised staff.

### 9. Allocation of email address and internet access

Users will be given an email address and shall regularly check their email boxes. Internet access is given to those who need to use these facilities as a normal part of their work. All email users will be issued with a unique password which shall be changed at regular intervals and shall be kept confidential by the user.

Accessing the email system using another employee's password without prior authorisation is a breach of policy and may result in disciplinary action in terms of the GEPF Disciplinary Code and Procedures.

### 10. Acceptable use of e-mail and internet

Email and internet usage shall be for GEPF business and support purposes only. Email services and internet browsing shall be used in a responsible manner and their use shall not adversely affect work performance.

The GEPF encourages the use of the internet and e-mail because they make communication more efficient and effective.

#### ❖ Legal considerations

In terms of the Data Protection Act, GEPF users shall take care that an email containing personal data:

- is not disclosed to unauthorised persons
- is only kept if it is required for work purposes, and
- Is kept secure at a place of work including printouts.

Users are responsible for managing their own records, i.e. protection from unauthorised access, filing records in an appropriate and organised manner and safeguarding against loss.

Information of a proprietary confidential nature shall not be disseminated or disclosed.

- It is the user's responsibility not to use any communication means such as the post, email or the internet for the creation or transmission of defamatory or libellous material.
- Intellectual property rights shall not be violated. Permission shall be sought from the copyright owner before sending or publishing copyrighted material.
- Users shall report to their line manager any suspected illegal or unauthorised use of GEPF email services or internet access.

### ❖ Security

It is important for users to be security conscious and to adhere to GEPF security procedures. The biggest threat to any computer system is unauthorised access. It is the user's responsibility not to leave their workstation unattended at any time once logged on to the GEPF's network.

- Users shall not use email or internet access facility to intentionally evade, or attempt to evade, the security/authentication mechanisms in existence.
- Access to email and the internet shall be authorised by user's line manager. When access has been given, passwords shall not be disclosed.
- Reports must be generated from time to time to view internet activity to establish patterns of misuse, abuse or threats and Incidents must be dealt with in accordance with this policy.

Size restrictions will be enforced on mailboxes and Users must manage their email facilities.

- Users shall use caution when opening email attachments or links received from unknown senders which may contain malicious software.
- Non-repudiation and integrity of messages must be ensured.
- All outgoing e-mail correspondence must include the following Information:
  - Name of sender;
  - Designation of sender;
  - Telephone number;
  - E-mail address; and
- A legal disclaimer vetted by the GEPF Legal Advice Unit must be automatically added to all outbound e-mails.

### **11. Unacceptable use of e-mail and internet**

Activities with any of the following characteristics are unacceptable:

- Under no circumstances may GEPF computers or other electronic equipment be used to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related internet sites. Doing so can lead to disciplinary action up to and including termination of employment.

# Confidential

## E-mail and Internet Policy

- Email and the internet shall not be used for the creation or transmission of any disruptive, offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.  
(Examples of forbidden transmissions, software, programmes or websites include , cartoons or jokes, unwelcome propositions or love letters, ethnic or racial slurs, or any other message that can be construed to be harassment or disparagement of others based on, inter alia, their sex, race, sexual orientation, age, national origin, or religious or political beliefs)
- Users are not to conduct personal business using the GEPF internet or email.
- Chain emails and the forwarding of non-business emails to friends, family and associates is not allowed.
- Viewing pornography or distributing pornographic material or stories via GEPF email infrastructure is not allowed.
- Violating the privacy of other users, i.e. obtaining without authorization the access codes and/or passwords of another user.
- Users are not allowed to forward email to communicate informal personal information, such as gossip, which may infringe upon the privacy of others, or for the transmission of material such, that infringes the copyright of another person.
- Users shall avoid sending anything that may be considered offensive, e.g. anything that may be considered racial, sexual or religious abuse.
- Users who experience any offensive email shall inform their line manager and Corporate Services immediately and such inappropriate behaviour will be treated seriously.
- Users are not allowed to download/ receive personal software by email or to download personal software from the Internet. Using the internet in a way that denies service to other users for example, deliberate or reckless overloading of access links or of switching equipment.
- Continuing to use an item of networking software or hardware after GEPF has requested that the user cease because it is causing disruption to the correct functioning of the Internet.
- Use of email or the internet to advertise, lobby, act as consultancy, design or carry out other commercial purposes.
- Email messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, and national origin, physical attributes or sexual preference.
- Viewing, storing, downloading or forwarding images, moving images, sound files, texts or recordings that are sexually explicit or sexually suggestive, harassing, intimidating or defamatory.
- Hacking in any form, including gaining or attempting to gain access to restricted resources either inside or outside of the GEPF's computer network.
- Software piracy or other infringement of intellectual property rights in digital content.
- The sending, whether on the internal email system or externally, of bulk unsolicited mail, commercial advertising of other businesses, mail-flooding, or excessive cross postings on newsgroups (called spam).
- The use of any computer resource to promote any business or enterprise, except that of the GEPF, unless such use is explicitly permitted by an agreement between the employee and the organisation.

- Issuing of unsolicited email to indicate or gain support for any religious or political purposes.
- GEPF Intranet and the internet must not be used for commercial marketing or private gain, distribution of chain letters or mass e-mails, or for the distribution and installation of illegal games, music or any unauthorized software.
- Users must be aware of the Risks and benefits of GEPF Intranet and internet usage.
- All connections between the GEPF internal networks and the internet must be secured connections.
- All Users must be identified and authenticated before accessing internet and Intranet resources.
- Usage of the internet must be reported on, monitored, controlled and managed.
- Content published to the internet and Intranet must be comply to the Communication policies
- All Users must be held responsible and accountable for their activities on the internet where, considering the particular facts of the matter, such activities amount to a disciplinary offence.
- Spending unauthorised and, or, extensive time on the internet, e-mail or other communications systems for non-business purposes is prohibited.
- Users may not use electronic mail, online services or internet facilities for unlawful or malicious activities.
- For any uses that violate other GEPF policies or guidelines.
- The email should be used according to the guideline in annexure A

### **12. Personal use of e-mail & internet facilities**

GEPF provides the electronic mail and internet system to assist users in the performance their duties, they shall use it for official/business purposes only. limited personal use of e-mail is permitted by the GEPF; however users shall not abuse this privilege. The personal use of emails will be treated the same as other messages undertaken for business/official purposes.

The GEPF reserves the right to access and disclose as necessary all messages sent over its e-mail system, without regard to content. Since users personal messages can be accessed by the GEPF without prior notice, users shall not use e-mail to transmit any messages they would not want to be comprehended by a third party.

### 13. General communications

- Each user is responsible for the content of all text, audio, programmes or images that they place retrieve or send over the GEPF's email/ 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 GEPF.
- All messages communicated on the GEPF's e-mail/internet system shall contain the employee's name.
- Any messages or information sent by an employee to another individual outside of the GEPF via an electronic network (e.g., bulletin board, online service or internet) are statements that reflect on the GEPF.
- Whenever using GEPF resources to access and use the internet and emails , users must realise that they represent the GEPF.
- Whenever Users acknowledge an affiliation to the GEPF, they must also clearly indicate that the opinions expressed are their own and not necessarily those of the GEPF
- All communications sent by users via the GEPF's e-mail/internet system shall comply with this and other GEPF policies and may not disclose any confidential or proprietary GEPF information.
- Notices, announcements or other messages pertaining to GEPF products or services may not be posted on public discussion groups, notice boards or bulletin boards without the express prior approval of the employee's line manager.
- Any unofficial communications found on the internet shall be communicated to the employee's line manager where such information may be found to be damaging to the image or infringe any rights of the GEPF.
- Each employee has a responsibility to use the electronic communication facilities and services in a lawful and informed and responsible way and in a manner, which conforms to network etiquette, custom, courtesy and GEPF policies.
- Furthermore, each employee shall use exactly the same standards of care and professionalism when using electronic communication facilities and services as they would when undertaking formal communication, e.g. writing a letter.

### 14. Monitoring e-mail use and internet access

All use of the email system and of internet access will be recorded and regularly monitored to ensure the system is being used effectively and in line with this policy and all relevant legislation. Users will be considered to have consented to this monitoring by their acceptance of an email address at GEPF and their agreement to comply with the GEPF policies.

Information Communication systems may be subject to periodic unannounced inspections, and shall be treated like other shared filing systems. All e-mail messages are GEPF records. The contents of e-mail, properly obtained for legitimate business purposes, may be disclosed within the GEPF without users' permission. Therefore, users shall not assume that messages are confidential. Back-up copies of e-mail may be maintained and referenced for business and legal reasons

All email messages and records of sites accessed will be retained within the GEPF for a reasonable period.

All email messages will be tracked on an on-going basis.

### **15. Virus protection**

All users are to ensure that their computer is enabled with the GEPF approved virus protection software where applicable. to avoid the transmission of malicious codes.

Users shall first scan hard drives and e-mail messages for resident viruses prior to accessing information on the hard drives and e-mail messages. Where a user suspects that an email message or an attachment, may contain a virus he/she is required to contact Corporate Services for assistance.

### **16. Functional responsibility**

The electronic mail system, including the computers, software licences, network, addresses and messages, whether stored or in transmission, is the property of the GEPF.

It is the responsibility of all users to comply with this policy and the reasonable expectations contained within.

Management will be responsible for managing the time and productivity output of subordinates with respect to abuse of the e-mail facility.

Management will have the final authority and ultimate accountability for granting access, prevention of abuse and appropriate adoption of the e-mail technologies.

Corporate Services will be responsible for the monitoring and auditing of the e-mail system.

Corporate Services will be responsible for the implementation of system related remedial actions.

### **17. Managements' accountability for e-mails used by their personnel**

Managers shall ensure that all their computer-using personnel, whether temporary, permanent or on contract, is made aware of the contents of this policy, and are required to apply the policy to all those who report to them. Managers are also accountable for their personnel to make use of the e-mail service.

### **18. Queries and clarification of policy**

Where an employee is uncertain as to the content of this policy, or requests further clarification issues, which are addressed in this policy they are required to contact the ICT for clarification.

### 19. Non-compliance and corrective action

In the event of non-compliance with, or breach of, any aspect of this policy, disciplinary action will be taken against Users in accordance with the GEPF's disciplinary policy, procedures and Board Charter.

Users shall be aware of their responsibilities to use GEPF's e-mail and internet for business purpose and to further the objective of the organization. Any user, who abuses the privilege of GEPF facilitated access to email or the internet, will be subject to corrective action in terms of the GEPF Disciplinary Code and Procedure. If necessary, the GEPF's also reserves the right to recover the monetary value of the cost of irresponsible use and abuse of email and internet facilities and to advise appropriate legal authorities of any illegal violations by user.

### 20. Policy review

Management will review the policy every three years and/or when significant legislative or procedure changes occur, to ensure the suitability, adequacy and effectiveness of the policy.

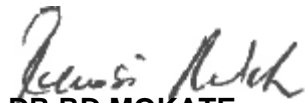
### 21. Approval

**RECOMMENDED / ~~NOT RECOMMENDED~~**



**Mr S MNGOMEZULU**  
**CHAIRPERSON: FINANCE AND AUDIT COMMITTEE**  
**DATE: 2020-06-10**

**APPROVED / ~~NOT APPROVED~~**



**DR RD MOKATE**  
**CHAIRPERSON: BOARD OF TRUSTEES**  
**DATE: 2020-06-10**

### Annexure A:

#### 22. Email Guidelines

The purpose of these guidelines is to provide users with email etiquette.

- Users shall always type in a concise subject title, sufficient to describe the content of the email, so that the recipient can delete or be alerted to the content without having to open the mail.
- Type messages in lower case for normal emails and only use upper case when there is a good reason e.g. when distinguishing replies from questions. Always use punctuation just as you would for written correspondence.
- Use the spell checking facility to correct misspellings prior to sending the email.
- Use the mailing lists already created to help them target the relevant audience more efficiently and effectively. Check that the recipient is included in the Mailing List to ensure the email goes to the intended group of recipients.
- Avoid sending very large attachments over the network. Documents which may cause particular problems include large files with photographic images, graphics or video clips. If in doubt shall contact the Corporate Services.
- Email is a messaging medium somewhere between a formal letter, memo and spoken or telephone communication. It tends to be more informal than the written word, but more formal than telephone conversations. Users shall, therefore, be very careful to avoid phrasing which may be misinterpreted or offend the recipient. The use of humour or irony does not always come across as intended and can cause offence.
- Anyone receiving an email which is clearly not meant to have been sent to them shall send it back to the originator as soon as possible.
- Emails shall not be forwarded on to another person without the permission of the originator, unless it is clear to any reasonable person that the information contained in the email is not intended to be in any way confidential.
- Email is not an appropriate debating forum. Users shall not use it to enter into discussion where it would be more appropriate to have a face to face meeting or to make contact by phone. Users shall not use it as a means of avoiding direct contact.
- Users can change the priority of an email to help the recipient assess its urgency.
- Critical information shall not be stored solely within the email system. Hard copies shall be kept or stored separately on the system