E-MAIL, SMS AND ELECTRONIC MESSAGING POLICY

CONTENTS

1 INTRODUCTION AND PURPOSE

IT EVOLUTION regards electronic messaging as a business tool for communicating with staff, customers, and suppliers.

Electronic messaging covers e-mail as well as different types of instant and store-and-forward messaging such as SMS texts, messaging apps, web chats and messaging facilities within social media platforms.

The purpose of this policy is to inform IT EVOLUTION employees how to use the electronic messaging tools provided by IT EVOLUTION and the rules applying to mobile devices used by you and other desktop computers used in the office.

Due to easy access and availability risks associated with all forms of electronic messaging must be minimised and avoided whenever possible.

The controls and best practices described in this policy apply to all employees, directors, board members, suppliers, third party service providers and any other persons who may have access to our systems and equipment from time to time.

The following policies and procedures also have relevance to this document:

- Acceptable Use Policy
- Anti-Virus and Malware Policy

2 SECTIONS OF THE POPI ACT ADDRESSED

Chapter 3 Condition 7 – Security Safeguards Section 19

3 E MAIL-SMS AND ELECTRONIC MESSAGING POLICY

3.1 Sending and Receiving of Electronic Messages

Only official facilities provided by our organisation may be used for official business. Personal e-mail accounts may not be used for sending or receiving business e-mails.

Any business electronic messaging, whether on your personal mobile device or otherwise, will always remain classified and considered to be the property of IT EVOLUTION and remain part of our official business and corporate records.

IT EVOLUTION, within the parameters of relevant legislation, retains the right to monitor and audit the use of electronic messaging, whether on company equipment or your own personal device.

Our Information Technology systems retain records of all official business communications and may be reviewed and audited by our duly authorised personnel.

Grammar and context are very important when using electronic messaging media and care should be taken not to be offensive in any way, while bearing in mind that different people and different cultures interpret communications differently. There are times it may be advisable to have a personal one on one telephone conversation with someone rather than use electronic messaging.

When dealing with classified information due care must be taken to ensure that persons who should not be privy to information may gain access to information, even by error or incorrect e-mail addresses being used.

Customer lists, employee data, accounting information and any other classified or sensitive information may only be sent and received on the company's official communication system.

Reputational harm which presents the potential to adversely affect our relationships with suppliers and customers can be easily caused via careless, external messaging.

Employees may not send electronic messages which are obscene or defamatory or which may not comply with our equality and diversity policies or which any recipient of a message sent by you may reasonably deem to be inappropriate.

If you are not certain as to whether your message may be inappropriate, or if you have a problem in the interpretation of this policy, please consult your line manager or departmental head.

4 PROHIBITED MESSAGING

IT EVOLUTION's accessible and official electronic messaging platforms and facilities may not be used under any circumstances for the following;

- for the distribution of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to any person or other organizations
- sending of material or correspondence that infringes the copyright or intellectual property rights of another person or organization.
- for activities that corrupt or destroy other users' data by way of virus infected correspondence
- to distribute any offensive, obscene, or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- to send any correspondence which may cause inconvenience, annoyance, or needless anxiety to any person.
- abusive, threatening, or bullying correspondence or messages
- to transmit material that encourages discrimination, or discriminates on the grounds of race, gender, sexual orientation, disability, political or religious beliefs.
- for activities that violate the privacy of others
- sending of anonymous messages without sender identification
- for any other activities which bring, or may bring, the organization into disrepute or cause reputational harm to IT EVOLUTION
- To "surf" the web for undesirable media, pornographic sites or web sites inciting racial or religious prejudice and violence.
- The organisations official communication channels and media may not be used to access Facebook or other social media you may use in personal capacity.

From a security perspective the best way to deal with spam or unsolicited junk mail is to delete them and never open the attachments, which may carry malware, or respond to such messages and junk mail. A request to the system administrator to block this e-mail domain from future communication.

4.1 Monitoring of Electronic Messaging Facilities

IT EVOLUTION advises you in this policy that electronic messaging is internally monitored and audited by duly authorised senior management employees of the business.

This is done to ensure that proper standards are maintained and to assess compliance with our own policies and procedures which are designed to ensure our organisations compliance with the POPI Act. Monitoring also assists us in detecting unauthorised access and potential crime.

If any employee suspects that our electronic messaging facilities are being abused by a user, they must contact the IT System administrator or Information Officer. All such reports will be investigated according to documented procedures and where appropriate, evidence provided. There is also a requirement to provide such information to regulatory or legislative bodies in accordance with the law.

The Information Officer or your departmental head may be approached by you if you have reason to suspect that our official channels of electronic communication are being used for non-business purposes.

You are instructed never to disclose your log on details or to use another staff member account for access to any of the organisations IT systems or infrastructure.

4.2 Using of Official Email

All e-mails sent from organization addresses to recipients outside of the organization will automatically carry the following disclaimer:

“The information contained in this e-mail and any files transmitted with it are confidential and intended for the addressee only. No other person is authorised to copy, forward, disclose, distribute or retain this email in any form. Whilst all reasonable steps are taken to ensure the accuracy and integrity of information and data transmitted electronically and to preserve the confidentiality thereof, no liability or responsibility whatsoever is accepted if information or data is, for whatever reason, corrupted or does not reach its intended destination. Please note any views expressed may be those of the originator and do not necessarily reflect those of this organisation. Furthermore, the contents of this mail are stated without prejudice and cannot be used against the sending party.”

Do not use auto-forwarding on emails e.g., whilst on holiday, if there is a possibility that this may result in classified information being forwarded to a recipient that does not have sufficient security clearance for the level of information involved.

Your mailbox will be configured with storage size limitations. This is to prevent available storage capacity being exceeded. If you notice difficulty with receiving of emails, please consult the system administrator before consulting any third-party service providers.

The general size limit on business emails and attachments are 36 MB and may be increased based on your role and work requirements in the company.

5 ANTI-VIRUS AND MALWARE

IT EVOLUTION has installed anti-virus software to protect our computer hardware that has network access from malware and virus’s. Please familiarise yourself with our Anti-Virus and Malware Policies.

Should you believe you have a virus please make contact as soon as possible with the System Administrator.

You may not perform any of the following actions while using official company communications platforms:

- Circulation of emails with the e-mail body or file attachments which you know to be infected with a virus, malware, or ransomware.
- download programs or data of any nature from unknown sources
- disable the installed anti-virus systems

The sending of a computer virus, malware, ransomware or malicious code from our organisation, whether accidental or not, is prohibited.

Declaration:

I confirm that I have read and understand the contents of this e-mail, SMS and electronic messaging policy and I undertake to abide with and comply with the requirements expected from me always when using the facilities provided by IT EVOLUTION.

Name: Date: / /20__

Signature: _____