

Email, Electronic Communication & Collaboration Policy

Document Classification	Confidential ☐ Internal ☐ Public ☒
--------------------------------	---

Email, Electronic Communication & Collaboration Policy

Table of Contents

1. Definitions	4
2. Executive Summary	5
3. Purpose	5
4. Objectives	5
5. Email, Electronic Communication & Collaboration Policy Introduction	6
6. Inappropriate use of company email	6
7. Appropriate use of corporate email and collaboration tools	6
8. Personal use	7
9. Email and Collaboration Security	7
10. Email signature	8
11. Disciplinary action	8
12. Policy Statement	8
13. Maintenance	8
14. Scope	8
15. Acknowledgement of Understanding	9

Email, Electronic Communication & Collaboration Policy

CHANGE CONTROL TABLE

No.	Revision	Status	Date	Author	Description of the change
1.	00.01	New	10/09/2018		Initial Document
2.	00.02	Reviewed	30/10/2018		Review
3.	00.03	Reviewed	09/11/2018		Updated
4.	00.04	Reviewed	15/11/2018		Review
5.	00.05	Reviewed	30/11/2018		Updated
6.	01.00	Released	16/01/2019		Released
7.	01.01	Reviewed	08/06/2021	JR McEndoo	Released
8.			Date		
9.			Date		
10.			Date		

DOCUMENT STATUS

No.	Status	Definition / Description
1.	New	New Document
2.	Reviewed	Document reviewed by Author and Management.
3.	Released	Document checked and released by Management. This document can only be modified if the version number is updated

VERSIONS

No.	Versions take place in two stages. Accepted documents receive the next higher integral version number.	
1.	00.01, 00.02 etc.	Not released versions, with the status "processed".
2.	01.00	First released version with the status "released".
3.	01.01, 01.02 etc.	Versions which supplement the version 01.00 and are "processed"
4.	02.00	Second released versions with the status "released".

Email, Electronic Communication & Collaboration Policy

DISTRIBUTION LIST

No.	Company	Name & Surname
1.	Social Path	Jessica Rose McEndoo
2.	Social Path	Charlotte Annie Wilhelm
3.	Social Path	Dorothy Constance Collett
4.	Social Path	Jana Elizabeth Doyle
5.	Social Path	Linda Monica Ceresa-Hall
6.	Connect Digital Mind	Olivia Dawn Bosman
7.	Social Path	Weronika Kinga Lukasiak
8.	Social Path	Lysandra Harding
9.	Qubi Solutions	Willie Cloete
10.	Emile Hay	Emile Hay

1. Definitions

Company:	Refers to Social Path (Pty) Ltd. (Social Path)
Confidential	Highly sensitive or valuable information, both proprietary and personal. Information, which is confidential by law or data if made public or even shared in an uncontrolled way around the Company, could seriously impede the Company's operations and therefore is considered critical to its on-going operations. Such information should not be copied or removed from the Company's operational control without specific authorisation from EXCO.
Employee:	Any person appointed on a company contract of employment, excluding independent contractors and persons employed by temporary employment services.
Internal	Information not approved for general circulation outside the Company where its loss would inconvenience the Company or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Disclosure of such data to anyone outside of the Company requires EXCO authorisation.
Public	Data or information that does not fall under any other classification levels and may be broadly distributed without causing damage to the Company, its employees, and stakeholders.
Event	An event is an exception to the normal operation of IT infrastructure, systems, applications, or services.
Incident	An incident is an event that violates the Social Path Computing Policy, Information Security Policy; or threatens the confidentiality, integrity, or availability of the Social Path Information Systems / Platforms or Services. "Information Security Incident" in the remainder of this policy and procedure document refers to an adverse event that has

Email, Electronic Communication & Collaboration Policy

	caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information technology resources and mediums, and the availability and continuity of critical information systems and processes.
	An Information Security Incident include, but are not limited to, the following types of scenarios: • Data Loss, Data Corruption or Data Theft, • Unauthorised exposure or leakage of company confidential information or data, • Unauthorised Access Attempts (either failed or successful) to access data, systems, platforms, or information storage. • Cyber Attacks including Denial Of Service (DoS), Distributed Denial of Service attacks (DDos), Man in the Middle Attacks, Malware, Spear Fishing, etc. • Changes to information or data or system hardware, firmware, or software characteristics without the Stakeholders' knowledge, instruction, or consent. • Any unauthorised changes to access permissions or privileges. • Any unauthorised use of any System or Service for the processing, storage or manipulation of data. • Unplanned / Unscheduled System, Service, Platform or Connectivity Outages / Service Disruptions • Severe System Performance or Functional Degradation

2. Executive Summary

This policy forms an integral part of the Social Path Information Security management methodology that aims to enforce governance and accountability for information security management across all the current and future Social Path owned, operated, or supported environments.

3. Purpose

The goal of the Email, Electronic Communication & Collaboration Policy is to provide the respective Social Path personnel, subcontractors, partners, and associates, guidance in terms of responsible usage of the Social Path Email, Electronic Communication and collaboration facilities, and the respective Social Path ICT assets utilised to perform any ICT related function across these mediums. The Key goal is to protect Social Path confidential data from breaches and safeguard our reputation and technological intellectual property.

4. Objectives

This policy aims to provide adequate guidance to govern responsible usage, this guidance aims to prevent any harm to individuals or the organisation and reduce the risk associated with the use of these mediums, to this end, all users and managers of Social Path information and IT systems are expected to:

- Understand their roles in providing the respective clarity and guidance to their respective personnel,
- Report any abuse, or breach of policy immediately to ensure that adequate corrective action can be taken.

This policy and the related Social Path policies and procedures provide a clear and consistent methodology to help to ensure that usage of any ICT related services, solutions or technology is adequately and consistently governed.

Email, Electronic Communication & Collaboration Policy

5. Email, Electronic Communication & Collaboration Policy Introduction

Corporate email, Instant messaging, voice and video conferencing and collaboration tools are powerful productivity enabling and enhancing tools that aim at assisting employees, contractors, and partners to communicate and collaborate efficiently from practically any internet connected device of geographic location.

These productivity tools however carry the risk of inadvertent exposure of confidential company information if not adequately secured and if not utilised responsibly, and further, carry the risk that the devices and credentials utilised to leverage these services can be compromised by attackers to gain access to confidential company information.

Employees, contractors, and partners must therefore apply adequate diligence in securing their devices, credentials as well as be cautious in terms of which of these mediums they utilise to share or collaborate on sensitive or confidential data. The Social Path corporate email and collaboration tools are therefore aimed primarily for work-related purposes.

Social Path, however, aims to provide employees with relative freedom to use their corporate email and collaboration services and tools for personal reasons, under the construct that all usage of corporate email, and the associated collaboration tools are used responsibly.

Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive or malicious content. Employees and users (herein referred to as "Users," or "User") accessing the Social Path email and collaborations tools do so at their own risk and understand and agree that Social Path (herein referred to as "Company," or "The Company") only condones legitimate, business, and personal responsible usage. To minimize the risks presented to these services and the data they manage by cyber threats, the use of the Social Path Corporate Email and Collaboration tools are governed by this Policy.

6. Inappropriate use of company email

All employees represent the company whenever they use their corporate email address or corporate collaboration tools.

They may therefore may not utilise these tools and services for the following:

- Signing up for illegal, unreliable, disreputable, or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Register for a competitor's services unless authorised.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their co-workers.
- Share any company confidential or propriety information or files.
- Share any sensitive data in instant messaging or collaboration portals including credit card or payment information.

NOTE] Social Path reserves the right to monitor, protect and archive corporate email communication for legislative and governance purposes.

7. Appropriate use of corporate email and collaboration tools

Employees are permitted to use their corporate email and collaboration tools for work-related purposes without limitations. For example, employees can use their email and the associated tools to:

- Communicate with current or prospective customers and partners.
- Schedule online or in person meetings, 1:1 or 1: Many
- Provide their email address and instant messaging addresses to people they meet at conferences, career fairs or other corporate events for business collaboration and communication purposes.
- Share files between authorised, trusted employees, contracts, and partners.
- Collaborate on new Company projects and initiatives.

Email, Electronic Communication & Collaboration Policy

- Manage project and/or service delivery initiatives.
- Sign up for newsletters, platforms and other online services that will assist them with their roles or professional growth.
- Attend online meetings and conferences that will assist them with their roles or professional growth.

8. Personal use

Employees are permitted to use their corporate email and collaboration tools for some personal purposes. For example, employees can use these tools to:

- Register for classes or meetups.
- Interact with their personal bank, insurance, medical or related service providers.
- Schedule online or in person personal meetings.
- Send emails to friends, family, and service providers if they do not generate or propagate spam or disclose any confidential information.

NOTE| Social Path reserves the right to monitor, protect and archive corporate email communication for legislative and governance purposes.

9. Email and Collaboration Security

Email is often the medium of cyber-attacks, confidentiality breaches and the medium most frequently exploited for the distribution of viruses and other malware. These issues can compromise the Social Path reputation, legality and the overall health and security of the Social Path ICT and digital assets.

To protect these assets and the associated services, all employees, contractors, and partners must therefore adhere to the following:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password every month. This is enforced by the email credential policy.
- Employees should always be vigilant and cautious when opening email as these, specifically unrecognised or unsolicited email, carry malware or phishing attacks. Employees should therefore:
 - Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
 - Be suspicious of clickbait titles or any unsolicited email or chat messages.
 - Check email and names of unknown senders to ensure they are legitimate.
 - Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If an employee is unsure that an email, they have received is safe, they can request assistance from the Social Path Management.
- The Social Path Email and Collaboration tools are protected by anti-malware, and targeted threat protection, including managed antivirus and patch management across all corporate ICT assets to provide an additional level of protection. These security mechanisms however may be bypassed if employees utilise their own personal services, such as Hotmail, Gmail or other free email services by adding these accounts to their corporate email client, adding these non-controlled, non-governed accounts to corporate assets are therefore prohibited.

Email, Electronic Communication & Collaboration Policy

- Employees must adhere to this policy at all times, in addition to the Social Path confidentiality and data protection guidelines.

10. Email signature

Social Path encourages employees to create an email signature that exudes professionalism and represents our company well. Executives and Salespeople, who represent the company to customers and stakeholders, must pay special attention to how they close a corporate email. The below depicts an example of an acceptable email signature:

- [Employee Name]
- [Employee Title], [Company Name with link]
- [Phone number] | [Company Address]
- Employees may also include the company logo and work-related videos and links in email signatures when this is applicable or suited to the respective email.

11. Disciplinary action

Employees who do not adhere to this policy will face disciplinary action up to and including termination of employment. Disciplinary action will therefore be taken under the following circumstances:

- Using a corporate email address to send confidential data without authorisation.
- Sharing company confidential information, code, applications, or license keys to unauthorised parties.
- Using email, collaboration, chat, or file sharing tools to distribute sensitive, confidential, or undesirable content.
- Sending offensive or inappropriate emails to our customers, colleagues, contractors, or partners.
- Using a corporate email, collaboration, chat, or file sharing tools for any illegal activities.

12. Policy Statement

Social Path will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information technology and/or the associated digital assets (data) within the custody of Social Path.

13. Maintenance

- The Social Path Executive and Information Security Personnel are responsible for the maintenance and revision of this Policy.
- This policy, and all related appendices, are reviewed as deemed appropriate or required, but no less frequently than every 12 months.
- This Policy review is undertaken by the Social Path Executive and Senior Management team.

14. Scope

This policy and procedures apply to the Platforms, Information Systems, Data, Services and Networks leveraged or utilised by Social Path and their respective service delivery partners and associates, including any person or device who gains access to these systems or data. The policy therefore applies to all Partners and Employees of Social Path, contractual third parties and representatives of Social Path who use Social Path IT services and solutions, or have access to, or custody of, customer information or Social Path proprietary information.

All Partners and Employees of Social Path, contractual third parties and representatives **must** therefore understand and adopt this policy, are responsible for ensuring the safety and security of Social Path systems and the information that they use or manipulate. All users have a role to play and a contribution to make to ensure that safe and secure use of the defined Social Path systems, services, platforms and associated technology, and the information that these environments contain.

Email, Electronic Communication & Collaboration Policy

15. Acknowledgement of Understanding

I have read and agree to comply with the terms of this policy governing the use of The Company's Email, Electronic Communication and Collaboration tools. I understand that violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties.

Printed Name:

Role / Designation

Signature:

Date: