ICT and Acceptable Usage Policy

Document Classification	**Confidential** ☐ **Internal** ☐ **Public** ☒

Table of Contents

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.	01.00	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”.

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

	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 ICT and Internet Acceptable Usage Policy is to provide the respective Social Path personnel, subcontractors, partners, and associates, guidance in terms of responsible access and usage of the Social Path networking and internet access facilities, and the respective Social Path ICT assets utilised to perform any ICT related function across these mediums.

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.

5. ICT and Internet Acceptable Usage Policy Introduction

Corporate ICT facilities including the provided wireless or cabled internet connectivity, Social Path corporate assets and any related ICT technology utilised by employees, contractors and partners utilised to perform the defined work-related functions for or on behalf of Social Path are mandated to abide by this policy. The key aim of this policy, aligned to the Social Path information security and governance methodology aims to provide clear guidance in terms of the acceptable usage of these ICT assets and the related services

6. Definitions

- **Electronic Device or Service**:
  - Internet, intranet, messaging (e.g. e-mail and instant messaging) or any other information delivery or exchange technology provided by Social Path or accessed by Social Path owned computers, including portable computers (Laptops or notebooks) and handheld devices such as Company-owned personal data assistants (PDAs), smartphones, cellular phones, or any respective computer applications.

- **Encryption**:
  - A mathematical process that converts the normal letters and words of an e-mail into a “secret code” that appears as unreadable to anyone except the person you sent the e-mail to who has the “secret key” to decipher the message.

- **Workstation:**
  - All Company-owned computers, including portable computers (laptops or notebooks) and desktops, as well as peripherals, such as printers, routers, facsimiles, and/or wireless network access cards, provided to employees for the purpose of conducting Company business. Also included are handheld devices such as Company-owned personal data assistants (PDAs) and smartphones.

7. STANDARDS / GUIDELINES

- Employees and other authorised persons may be granted access to workstations and other electronic devices or services in order to perform their duties. (People granted such access are referred to in this policy as “Users”.) Such access is discretionary on the part of the Company and may be revoked at any time and is subject to the Company’s related information security policies.

- Passwords are provided to and/or setup by the employee to provide job-specific access to programs and systems. These passwords are to be always kept confidential and thereby the employee agrees not to use another employee’s password or provide an employee with his/her password to access these systems. Only authorised IT support personnel may have access to passwords to provide support for a limited, controlled duration post which these passwords must be reset so they are only known by the “User”.

- At any time, management can request access to any electronic user files, including e-mail messages, instant messaging logs and cellular phone text messages on Company email and equipment provided for work purposes.

- The use of encryption keys and certificates (strings of characters used for encryption/decryption) where applicable is mandated. All keys and certificates required to decrypt Company-owned information must be provided upon request by management, and carefully managed by the respective, authorised staff.

8. Use of Computers and Other Electronic Tools and Services

- Electronic devices or services are extensions of the workplace. Abuse or inappropriate use of electronic devices or services will subject an employee to disciplinary procedures under Social Path' s disciplinary process up to and including possible termination of employment.
- Employees may not use the Social Path e-mail or collaboration tools, services, and systems for the distribution of computer games or other computer novelty items that are not work related.
- Social Path reserves the right to audit Company owned computer equipment and any other electronic devices or services on a periodic basis to ensure compliance with this policy.
- It is not acceptable to use a Social Path provided workstation from any location for any activities that do not relate to the business of the Company, including, but not limited to, the following:
  - Transmitting, downloading, storing, or displaying any materials, messages, content, or correspondence that the Company deems derogatory, defamatory, threatening, obscene, insulting, pornographic, including sexually explicit images, messages or communications containing racial or ethnic slurs or anything that might be construed as harassment or offensive to others based on race, colour, religion, gender, age, national origin, disability, citizenship or veteran status, or any other legally protected category.
  - Distributing Company, Employee, Partner or Customer information without appropriate authorisation.
- Uploading, downloading, or installing software, unless it relates to the users' official assignments and/or job responsibilities, and appropriate authorisation has been obtained.
- Illegally downloading or otherwise copying any electronic media is strictly prohibited.
- Downloading any software or electronic files without reasonable virus protection measures in place. Furthermore, employees should ensure that no viruses are brought into the system by downloading potentially damaging material or transferred to computer or network by means of a USB device.
- Employees shall not make or use illegal copies of copyrighted material, store such material on Company equipment, or transmit such material over the Company network.
- Intentionally interfering with the normal operation of the Company's perimeter firewall or related security mechanism.
- Altering the settings of, removing, or disabling, any software installed by the Company without prior authorisation.
- Accessing data stored on Company's computer equipment from outside the Company that is not for purposes of conducting your duties (e.g. accessing records from a home computer), unless expressly authorised by the Company.
- Attempting any unauthorized access to electronic information or systems.
- Intentionally reading or disclosing the content of e-mail that was not directed to the employee.
- The Company's intranet or Internet connections shall not be used for non Social Path commercial or political purposes.
- Employees shall not use Company network for personal gain such as selling access of a Company user login ID.
- Internet access through the Company network shall not be used for performing unauthorised work for profit.
- Use of any Company resources for illegal and personal activity is grounds for progressive discipline, up to and including termination. Should any such activity occur, the Company is mandated to report the employee to the appropriate authorities in accordance with the law.
- All data, information, work, product, and correspondence created on a workstation is the property of the Company.
- All data sent, received, or stored on the Company's computer equipment shall be and remain the property of the Company.
- By using a Company workstation or electronic device or service, the employee expressly consents to monitoring by Social Path, agrees to comply with all limitations on the use of Company equipment and electronic devices or services, and understands that such equipment and services are not private.

- Social Path will periodically review, track, and monitor workstation and electronic devices or services usage to determine compliance with this policy, the Company will review alleged violations of this policy on a case-by-case basis. All messages on the e-mail system are traceable to their author even after they are "deleted"
- Social Path has implemented solutions to log and monitor all internet access and usage.
- Internet/Intranet activity and all electronic services may be subject to discovery orders in litigation matters.
- The provisions of this policy, including any monitoring or inspection, may be implemented without warning or notice.
- Violations of this policy will result in disciplinary action, up to and including termination of employment.

9. DISCIPLINARY ACTION

The following general guidelines may be used for the purposes of taking disciplinary action against employees.

ACCEPTABLE USE OFFENCES

The following general guidelines may be used for the purposes of taking disciplinary action against employees

Category	Type of Offence	1ST d Occurrence	2ND Occurrence	3RD Occurrence
1. Loading illegal software or offensive material onto a Company computer. Wilful or negligent introduction of a virus into an employee's computer or any other computer system in the Company.	Serious	Final written warning or hearing	Immediate dismissal	
2. Use of electronic mail, online services, internet facilities and services, and the world wide web for unlawful or malicious activities. Use of abusive or objectionable language in either public or private communication. Misrepresentation of oneself or inappropriate representation of Social Path.	Serious	Final written warning or hearing	Immediate dismissal	
3. Negligent misconduct in relation to computers and software technology. Intentional or grossly negligent damage to computer hardware or software of the Company or an employee.	Serious	Final written warning or hearing	Immediate dismissal	
4. Activities that cause congestion and disruption of Social Path's networks and systems.	Serious	Written warning	Final written warning or hearing	Immediate dismissal
5. Spending unauthorised and/or extensive time on the internet, email or other communications systems for non-business purposes.	Serious	Written warning	Final written warning or hearing	Immediate dismissal
6. Accessing pornographic or discriminatory material, use of electronic mail for communications that contain improper or unlawful statements including but not limited to ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on race, national origin, sex, sexual orientation, age, disability, or religious beliefs; or communications that contain sexually explicit or offensive images, cartoons, graphics, sound or text. Viewing, downloading, copying, storing and/or distributing undesirable, indecent and/or obscene graphics, images, cartoons, sound or	Serious	Verbal warning	Written warning	Final written warning or hearing and or Immediate dismissal

text from email, the internet, the world wide web or any data storing utility on the Company's computer system and/or network.				
7. Changing the configuration of computer hardware or software without proper authorization.	Serious	Verbal warning	Written warning	Final written warning or hearing and or Immediate dismissal
8. Removing a computer, software, or hardware from Company premises without authorisation.	Serious	Verbal warning	Written warning	Final written warning or hearing and or Immediate dismissal
9. Purchasing computer equipment without proper authorisation.	Serious	Written warning	Final written warning or hearing	Immediate dismissal
10. Contracting for the development of computer software or related services without proper authorisation.	Serious	Written warning	Final written warning or hearing	Immediate dismissal
11. Accessing information available on Company computers or networks to which you are not properly authorised. For example, attempts to "hack" into other systems or another person's login, "crack" passwords, breach computer or network security measures, or monitor electronic files or communications of other employees or third parties except by the explicit direction of management. Divulging of allocated usernames and/or password to any third party or coemployee or allowing a coemployee or third party to use the username and/or password; Unauthorised use of an employee's terminal or a coemployee's terminal; Unauthorised use of private software on Company PCs, downloading and unauthorised copying of Company and other software for home and external use.	Serious	Final written warning or hearing	Immediate dismissal	

10. Queries and Clarification of Policy

Where an employee is uncertain as to the content of this policy, or requests further clarification on issues which are addressed in this policy, they are required to contact their department manager, the HR Department or the CEO/MD for clarification.

11. Use of Computers, Hardware and Related Company Assets

- Computers, hardware, software, and related Company assets must be safeguarded against environmental hazards (dust, excessive heat, damp, lightning, etc.), and unauthorised use always.
- As with other Company assets, no computer hardware or software may be removed from the Company's premises without authorisation from the employee's manager/supervisor.
- Laptops and other moveable computer devices must be locked away or secured when the employee is away from his/her work area. While an employee is away on extended absence from the workplace, not making use of such devices, or on leave, devices must be handed in to the Department Manager or IT Department for safekeeping.

- Purchases of all computer hardware, software, and peripheral hardware must be approved by the employee's Departmental Manager and the CEO/MD in accordance with Company purchasing procedures.
- All computer, hardware and software problems must be reported to the authorised IT support personnel.

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, is 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 safe and secure use of the defined Social Path systems, services, platforms and associated technology, and the information that these environments contain.

15. Acknowledgement of Understanding

I have read and agree to comply with the terms of this policy governing the acceptable usage of The Company's ICT and Internet Services. 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: _____