SOLUTIONPATH

Acceptable Use Policy

1 Overview

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Solutionpath' established culture of openness, trust and integrity. We are committed to protecting Solutionpath' employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, Office 365 and associated storage, internet browsing, and FTP, are the property of Solutionpath. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Solutionpath employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

1.1 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Solutionpath. These rules are in place to protect the employee and Solutionpath. Inappropriate use exposes Solutionpath to risks including virus attacks, compromise of network systems and services, and legal issues.

1.2 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Solutionpath business or interact with business systems, whether owned or leased by Solutionpath, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Solutionpath are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Solutionpath policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Solutionpath, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Solutionpath.

2 Policy

2.1 General Use and Ownership

Solutionpath proprietary information stored on electronic and computing devices whether owned or leased by Solutionpath, the employee or a third party, remains the sole property of Solutionpath.

You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Act 2018 and associated UK General Data Protection Regulations (UK GDPR).

You have a responsibility to promptly report the theft, loss or unauthorised disclosure of Solutionpath proprietary information.

You may access, use or share Solutionpath proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

For security and network maintenance purposes, authorised individuals within Solutionpath may monitor equipment, systems and network traffic at any time.

Solutionpath reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.2 Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with the following:

a) System level and user level passwords must comply with the document. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
b) All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended.
c) Postings by employees from a Solutionpath email address to forums or other such online sites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Solutionpath, unless posting is in the course of business duties.
d) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

2.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Solutionpath authorised to engage in any activity that is inappropriate (e.g. accessing gambling or pornographic websites), or deemed illegal under local, national or international law while utilising Solutionpath owned resources (including BYOD devices used to access the organisations information assets).

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

2.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Solutionpath.
b) Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Solutionpath or the end user does not have an active license is strictly prohibited.
c) Accessing data, a server or an account for any purpose other than conducting Solutionpath business, even if you have authorised access, is prohibited.
d) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
e) Introduction of malicious programs into the Solutionpath digital environment (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
f) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
g) Using a Solutionpath computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
h) Making fraudulent offers of products, items, or services originating from any Solutionpath account.
i) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
j) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
k) Port scanning or security scanning is expressly prohibited unless prior notification is given to the Technical Operations Manager.

l) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
m) Circumventing user authentication or security of any host, network or account.
n) Introducing honeypots, honeynets, or similar technology on the Solutionpath network.
o) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
p) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
q) Providing information about, or lists of, Solutionpath employees to parties outside Solutionpath.

2.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realise they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the Director IT Operations. The following are prohibited:

a) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Exceptions may be made for marketing purposes.
b) Any form of harassment via email, telephone, whether through language, frequency, or size of messages.
c) Unauthorised use, or forging, of email header information.
d) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
e) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type. This includes forwarding emails that look legitimate such as virus warnings. The majority of this type of email you will receive will be a hoax which you are further propagating by sending it on however well intentioned. If in doubt, speak to the Director IT Operations.
f) Use of unsolicited email originating from within Solutionpath' networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Solutionpath or connected via Solutionpath' network.

2.3.3 Blogging and Social Media

Blogging by employees, whether using Solutionpath' property and systems or personal computer systems, is also subject to the terms and restrictions set forth

in this Policy. Limited and occasional use of Solutionpath' systems to engage in blogging is acceptable, provided:

1) That it is done in a professional and responsible manner;
2) Does not otherwise violate Solutionpath' policy,
3) Is not detrimental to Solutionpath' best interests; and
4) Does not interfere with an employee's regular work duties.

Blogging from Solutionpath' systems is also subject to monitoring. Solutionpath' Information Security Policy also applies to blogging. As such;

a) Employees are prohibited from revealing any company confidential or proprietary information, trade secrets or any other material covered by Solutionpath' Information Security policy when engaged in blogging.
b) Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Solutionpath and/or any of its employees.
c) Employees are prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Solutionpath'
d) Employees may not attribute personal statements, opinions or beliefs to Solutionpath when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Solutionpath.
e) Employees assume any and all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Solutionpath' trademarks, logos and any other Solutionpath intellectual property may also not be used in connection with any blogging activity

3 Policy Compliance

3.1 Compliance Measurement

The ISO team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

3.2 Exceptions

Any exception to the policy must be approved by the Director IT Operations' team in advance.

3.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4 Related Standards, Policies and Processes

- POL – Information Security Policy Statement
- 1.1 Complaint Policies Document
- 9.2 User Access Management and Responsibilities
- 9.3 System and Application Access Control

5 Authorisation and Amendment Record

Document Prepared by:	**Document Authorised by:**	**Review Date**
Director IT Operations	Richard Gascoigne	See Audit Schedule

Version Number	**Amendment Made**	**Date of Issue**
1.0	Document Released	05/01/2021
1.01	Brand 21 Updates	18/10/2021
1.02	Review and update 4 “Issue” now “Version”	02/10/2022
1.03	Review, Formatting and updates to 2.2, 2.3, 4, 5 document owner at 2.3.2, 3.2 and 5	04/10/2023