Acceptable Use Policy

**Classification**: Internal

This document may only be shared internally without prior confirmation from the owner.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Approved By | Owner | Date Last Updated | Review Frequency | Next Review | Comments |
|  |  |  |  |  |  |  |

Contents

[Purpose of This Document 1](#_Toc142819499)

[Scope 2](#_Toc142819500)

[Responsibilities 2](#_Toc142819501)

[Exceptions 2](#_Toc142819502)

[Computer Access Control 2](#_Toc142819503)

[Internet & Email Use 2](#_Toc142819504)

[Clear Desk & Screen 3](#_Toc142819505)

[Remote Working 3](#_Toc142819506)

[Mobile Storage Devices 3](#_Toc142819507)

[Transferring Data 3](#_Toc142819508)

[Software 3](#_Toc142819509)

[Malware 3](#_Toc142819510)

[Telephony (Voice) Equipment 4](#_Toc142819511)

[Actions upon Leaving the TechSolution.inc 4](#_Toc142819512)

[Monitoring and Filtering 4](#_Toc142819513)

# Purpose of This Document

This document provides guidance on using IT assets appropriately to prevent data breaches.

# Scope

This Acceptable Use Policy applies to.

* TechSolution.inc’s IT equipment and information security.
* Use of email, internet, voice, and mobile devices.
* All TechSolution.inc business-related information.

# Responsibilities

**Line Managers**

* Line Managers must ensure that individuals are given clear direction on the extent and limits of their authority concerning IT systems and data.
* Ensure staff, temporary employees, contractors and secondees will comply with this policy
* Recover TechSolution.inc devices from departing staff or those not needing them.
* Grant access to data and systems based on genuine need.
* Revoke access for departing staff or those not needing it.
* Clarify individual authorities regarding IT and data

**All Staff**

* Comply with this and related policies.
* Report suspected policy breaches to line managers or IT.

**Exceptions**

* Seek exceptions through the IT Helpdesk.

# Computer Access Control

* Keep login details confidential.
* Consult IT before connecting non-TechSolution.inc devices, except for the ‘Guest’ network.
* Obtain approval before sharing TechSolution.inc data externally.

# Internet & Email Use

* Personal use is allowed if it doesn’t affect work, harm TechSolution.inc, or breach employment terms or legal obligations.
* Personal use is permitted where such use does not affect the individual’s business performance, is not detrimental to TechSolution.inc in any way, is not in breach of any term and condition of employment, and does not place the individual or TechSolution.inc in breach of statutory or other legal obligations.
* Get permission before publishing TechSolution.inc-related information online.
* Don't email private TechSolution.inc data to personal accounts, except payslips/P60s.
* Avoid offensive or inappropriate communications.
* TechSolution.inc IT shouldn't be used for personal gain.
* Respect copyright for downloaded material.

# Clear Desk & Screen

* Don't leave confidential data unattended.
* Lock computers when away.
* All business-related printed matter must be disposed of using confidential waste bins or shredders.

# Remote Working

* Safeguard TechSolution.inc devices in public and during travel.
* Don't share devices with non-TechSolution.inc employees.
* Avoid unsecured and unfamiliar wi-fi.
* Protect mobile devices with strong passwords and encryption.
* Particular care should be taken with mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password/passphrase in line with the Password Guidelines or a PIN and, where available, encryption.

# Mobile Storage Devices

* Use USB and external drives only when necessary.
* Encrypt confidential data on such devices.
* Devices should not be shared with non-employees.

# Transferring Data

* Ensure confidential data is always encrypted and that the decryption key or password is sent through a separate form of communication.

# Software

* Follow software licensing agreements.
* Employees are not permitted to install any software on systems without prior approval from the IT Department.
* Maintain proof of ownership for TechSolution.inc data in third-party software.

# Malware

* Don't bypass the security measures designed to protect our organisation, including.
  + Anti-Virus Software - All PCs have antivirus software installed to detect and remove viruses automatically.
  + Mimecast – This scans incoming and outgoing emails for potentially harmful threats.
  + Anti-Ransomware – Software which protects infrastructure from external attacks that lock owners out of technology in exchange for payments.
  + Web-Filtering – To ensure that websites are appropriately filtered and content is safe.

# Telephony (Voice) Equipment

* Refer to the TechSolution.inc Mobile Phone Policy when issued a TechSolution.inc phone.
* Avoid inappropriate calls.
* Accept reverse charge calls only for business reasons.

# Actions upon Leaving the TechSolution.inc

* Return all TechSolution.inc assets.
* All TechSolution.inc data or intellectual property developed or gained during the period of employment remains the property of TechSolution.inc. It must not be retained beyond termination or reused for any other purpose.

# Monitoring and Filtering

* TechSolution.inc owns all data on its computers but will try not to open personal emails.
* System activity may be monitored for security and misuse.
* Monitoring follows UK laws and local regulations for non-UK staff.
* Audited controlled internal processes will do any monitoring, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000. If this policy contradicts local regulations for staff outside of the UK, local statutory requirements will apply.