INSERT LOGO

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

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

INSERT LOGO

Scope

This Acceptable Use Policy applies to;

- [Company Name]'s IT equipment and information security;
- Use of email, internet, voice, and mobile devices;
- All [Company Name] 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 [Company Name] 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-[Company Name] devices, except for the 'Guest' network;
- Obtain approval before sharing [Company Name] data externally.

Internet & Email Use

- Personal use is allowed if it doesn't affect work, harm [Company Name], 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 [Company Name] in any way, is not in breach of any term and condition of employment, and does not place the individual or [Company Name] in breach of statutory or other legal obligations.
- Get permission before publishing [Company Name]-related information online;
- Don't email private [Company Name] data to personal accounts, except payslips/P60s;
- Avoid offensive or inappropriate communications;

- [Company Name]'s 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 [Company Name] devices in public and during travel;
- Don't share devices with non-[Company Name] 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 [Company Name] 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 [Company Name] Mobile Phone Policy when issued a [Company Name] phone;
- Avoid inappropriate calls;
- Accept reverse charge calls only for business reasons.

Actions upon Leaving the [Company Name]

- Return all [Company Name] assets;
- All [Company Name] data or intellectual property developed or gained during the period of employment remains the property of [Company Name]. It must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

- [Company Name] 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.