**Acceptable Usage Policy**

This Acceptable Usage Policy covers the security and use of information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all employees, contractors and agents (hereafter referred to as ‘individuals’).

This policy applies to all information, in whatever form, relating to business activities worldwide, and to all information handled by business relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated by business or on its behalf.

**Computer Access Control – Individual’s Responsibility**

Access to the business IT systems is controlled using User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the (Acme Corporation’s) IT systems.

**Individuals must not:**

* Allow anyone else to use their user ID/token and password on any business IT system.
* Leave their user accounts logged in at an unattended and unlocked computer.
* Use someone else’s user ID and password to access (Acme Corporation’s) IT systems.
* Leave their password unprotected (for example writing it down).
* Perform any unauthorized changes to (Acme Corporation’s) IT systems or information.
* Attempt to access data that they are not authorized to use or access.
* Exceed the limits of their authorization or specific business need to interrogate the system or data.
* Connect any non-business authorized device to the business network or IT systems.
* Store business data on any non-authorized business equipment.
* Give or transfer business data or software to any person or organization. outside business without the authority of business.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority regarding IT systems and data.

**Internet and email Conditions of Use**

Use of business internet and email is intended for business use. Personal use is permitted where such use does not affect the individual’s business performance, is not detrimental to business in any way, not in breach of any term and condition of employment and does not place the individual or business in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

**Individuals must not:**

* Use the internet or email for the purposes of harassment or abuse.
* Use profanity, obscenities, or derogatory remarks in communications.
* Access, download, send or receive any data (including images), which business considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
* Use the internet or email to make personal gains or conduct a personal business.
* Use the internet or email to gamble.
* Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
* Place any information on the Internet that relates to business, alter any information about it, or express any opinion about business, unless they are specifically authorized to do this.
* Send unprotected sensitive or confidential information externally.
* Forward business mail to personal (non-Acme Corporation) email accounts (for example a personal Hotmail account).
* Make official commitments through the internet or email on behalf of business unless authorized to do so.
* Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
* In any way infringe any copyright, database rights, trademarks or other intellectual property.
* Download any software from the internet without prior approval of the IT Department.
* Connect business devices to the internet using non-standard connections.

**Clear Desk and Clear Screen Policy**

In order to reduce the risk of unauthorized access or loss of information, business enforces a clear desk and screen policy as follows:

* Personal or confidential business information must be protected using security features provided for example secure print on printers.
* Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
* Care must be taken to not leave confidential material on printers or photocopiers.
* All business-related printed matter must be disposed of using confidential waste bins or shredders.

**Working Off-site**

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

* Working away from the office must be in line with business remote working policy.
* Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
* Laptops must be carried as hand luggage when travelling.
* Information should be protected against loss or compromise when working remotely (for
* example at home or in public places). Laptop encryption must be used.
* Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

**Mobile Storage Devices**

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only business authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

**Software**

Employees must use only software that is authorized by business on (Acme Corporation’s) computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on business computers must be approved and installed by the business IT department.

**Individuals must not:**

* Store personal files such as music, video, photographs or games on business IT equipment.

**Viruses**

The IT department has implemented centralized, automated virus detection and virus software updates within the business. All PCs have antivirus software installed to detect and remove any virus automatically.

**Individuals must not:**

* Remove or disable anti-virus software.
* Attempt to remove virus-infected files or clean up an infection, other than using approved business anti-virus software and procedures.

**Telephony (Voice) Equipment Conditions of Use**

Use of business voice equipment is intended for business use.

Individuals must not use business voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual’s own expense using alternative means of communications

**Individuals must not:**

* Make hoax or threatening calls to internal or external destinations.
* Accept reverse charge calls from domestic or International operators, unless it is for business use.

**Actions upon Termination of Contract**

All business equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to business at termination of contract.

All business data or intellectual property developed or gained during the period of employment remains the property of business and must not be retained beyond termination or reused for any other purpose.

**Monitoring and Filtering**

All data that is created and stored on business computers is the property of business and there is no official provision for individual data privacy, however wherever possible business will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. business has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

**It is your responsibility to report suspected breaches of security policy without delay to your line management, the IT department, the information security department or the IT helpdesk.**

**All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with business disciplinary procedures.**

*https://www.getsafeonline.org/themes/site\_themes/getsafeonline/download\_centre/sample\_acceptable\_usage\_policy.pdf*