

## **Acceptable ICT Usage Policy**

This document should be tailored to your organisation's specific requirements.

This Acceptable Usage Policy covers the security and use of all (Customer Names) Information and IT equipment. It also includes email, internet, voice and mobile IT equipment. This policy applies to all (Customer Name's) employees, contractors, and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to (Customer Names) Business activities worldwide, and all information handled by (Customer Name) relating to other organisations with whom it deals.

It also covers all IT and information communications facilities operated by (Customer Name) or on its behalf.

### **Computer Access Control – Individual's Responsibility**

Access to the (Customer Name) IT systems is controlled by the use of 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 (Customer Name's) IT systems.

#### **Individuals must not:**

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

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 (Customer Name) 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 (Customer Name) in any way, is not in breach of any term and condition of employment and does not place the individual or (Customer Name) 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 (Customer Name) considers offensive in any way, including sexually explicit, discriminatory, Defamatory or libellous 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 (Customer Name), alter any information about it, or express any opinion about (Customer Name), unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward (Customer Name) mail to personal (non-Customer Name) email accounts (for example, a personal Hotmail account).
- Make official commitments through the internet or email on behalf of (Customer Name) unless authorised.
- downloadedad 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 (Customer Name) devices to the internet using non-standard connections.

### **Clear Desk and Clear Screen Policy**

In order to reduce the risk of unauthorised access or loss of information, (Customer Name) 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 not to 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 comply with (Customer Name) 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 (Customer Name) authorised mobile storage devices with encryption enabled must be used when transferring sensitive or confidential data.

### **Software**

Employees must use only software that is authorised by (Customer Name) on (Company Names) computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on (Customer Name) computers must be approved and installed by the (Customer Name) IT department.

#### **Individuals must not:**

- Store personal files such as music, video, photographs, or games on (Customer Name) IT equipment.

### **Viruses**

The IT department has implemented centralised, automated virus detection and virus software updates within the (Customer Name). 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 by the use of approved (Customer Name) anti-virus software and procedures.

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

Use of (Customer Name) voice equipment is intended for business use. Individuals must not use (Customer Name's) 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 communication.

**Individuals must not:**

- Use (Customer Name's) voice for conducting private business.
- 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 (Customer Name) equipment and data, for example, laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to (Customer Name) at the termination of the contract.

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

**Monitoring and Filtering**

All data that is created and stored on (Customer Name) computers is the property of (Customer Name), and there is no official provision for individual data privacy, however, wherever possible, (Customer Name) 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. (Customer Name) has the right (under certain conditions) to monitor activity on its systems, including internet and email use, 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 NZ Data Protection Act the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 1998

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 (Acme Corporation) disciplinary procedures.