ICT Acceptable Usage Policy

Introduction

This Acceptable Usage Policy covers the security and use of all Best Practice Training & Development Ltd information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all employees, contractors, agents and learners (hereafter referred to as 'individuals').

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

Individuals must not:

- Allow anyone else to use their user ID/token and password on any IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to IT systems or information.
- Attempt to access data that 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-Best Practice authorised device to network or IT systems.
- Store Best Practice data on any non-authorised equipment.
- Give or transfer Best Practice data or software to any person or organisation outside without the authority of Best Practice.
- Access or download any illegal or obscene information or images.

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

Internet and email Conditions of Use

Use of Best Practice 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 Best Practice in any way, not in breach of any term and condition of employment and does not place the individual or Best Practice in breach of statutory or other legal obligations.

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

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Best Practice 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 Best Practice 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 Best Practice 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 Best Practice on Best Practice) computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Best Practice computers must be approved and installed by the Best Practice IT department.

Individuals must not:

- Store personal files such as music, video, photographs or games on Best Practice IT equipment.

Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within the Best Practice. 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 Best Practice anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

Use of Best Practice voice equipment is intended for business use. Individuals must not use Best Practice 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:

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

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

Monitoring and Filtering

All data that is created and stored on Best Practice computers is the property of Best Practice and manages a perimeter firewall between its' Internet connection to establish a secure environment for computer resources. This firewall filters Internet traffic to mitigate the risks and potential losses associated with security threats to the network and information systems. In addition the firewall secures a number of other 'zones' controlling traffic between clients and servers and other parts of the data network.

IT system logging will take place where appropriate, and investigations will be commence where reasonable suspicion exists of a breach of this or any other policy. Best Practice 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.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 2018

It is your responsibility to report suspected breaches of security policy without delay to your line management, Quality Manager or Managing Director.

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

Date of Policy – 14.01.2019
Review date - 14.01.2020