IT Acceptable Usage Policy

This Acceptable Usage Policy covers the security and use of all Tower Learning Centre's information and IT equipment. It also includes the use of email, internet and IT equipment. This policy applies to all Tower Learning Centre employees, including non-contracted staff.

This policy applies to all information, in whatever form, relating to Tower Learning Centre business activities, and to all information handled by Tower Learning Centre relating to other organisations with whom it deals.

Computer Access Control – Individual's Responsibility

Access to the Tower Learning Centre systems are controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Tower Learning Centre IT systems.

Individuals must not:

- Allow anyone else to use his or her password on any Tower Learning Centre IT system
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Tower Learning Centre IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Tower Learning Centre 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- Tower Learning Centre authorised device to the Tower Learning Centre network or IT systems.
- Store Tower Learning Centre data on any non-authorised Tower Learning Centre equipment.
- Give or transfer Tower Learning Centre data or software to any person or organisation outside Tower Learning Centre without the authority of Tower Learning Centre

Internet and email Conditions of Use

Use of Tower Learning Centre 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 Tower Learning Centre in any way, not in breach of any term and condition of employment and does not place the individual or Tower Learning Centre 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 Tower Learning Centre 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 Tower Learning Centre alter any information about it, or express any opinion about Tower Learning Centre, unless they are specifically authorised to do this.
• Send unprotected sensitive or confidential information externally.
• Forward Tower Learning Centre mail to personal non- Tower Learning Centre email accounts (for example a personal Hotmail account).
• Make official commitments through the internet or email on behalf of Tower Learning Centre unless authorised 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 Tower Learning Centre devices to the internet using non-standard connections.

Clear Desk and Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Tower Learning Centre enforces a clear screen policy as follows:

• 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.

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 Tower Learning Centre 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 Tower Learning Centre on Tower Learning Centre computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Tower Learning Centre computers must be approved and installed by the Tower Learning Centre IT department.

Individuals must not:

• Store personal files such as music, video, photographs or games on Tower Learning Centre IT equipment.

Viruses

The IT department has implemented an, automated virus detection and virus software updates within Tower Learning Centre. 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 Tower Learning Centre anti-virus software and procedures.

Telephone Equipment Conditions of Use

Use of Tower Learning Centre telephone equipment is intended for business use

Individuals must not:

• Use Tower Learning Centre voice for conducting private business.
• Make hoax or threatening calls to internal or external destinations.
• Accept reverse charge calls from domestic or International operators

Actions upon Termination of Contract

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

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

Monitoring and Filtering

All data that is created and stored on Tower Learning Centre computers is the property of Tower Learning Centre and there is no official provision for individual data privacy, however wherever possible Tower Learning Centre 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. Tower Learning Centre 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 1998

It is your responsibility to report suspected breaches of security policy without delay to Kate Towers or David Ratcliff

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

Name: _____ Signed: _____

Date: _____