**IT Acceptable Usage Policy**

December 2019

**Purpose**

Daniel Thwaites Plc ("the Company") operates the following policy in relation to the security and use of all Thwaites information and IT equipment by all employees. It also includes the use of email, internet, voice and mobile IT equipment.

The purpose of the Acceptable Usage Policy covers the security and use of all Thwaites information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Thwaites employees, contractors and agents (hereafter referred to as ‘individuals’). It applies equally to all employees regardless of their age, sex, marital or civil partnership status, racial or ethnic group, disability, sexual orientation, religion or belief.

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

**Scope**

The policy is a guide only and not contractual and applies to all employees within the Thwaites group of companies.

Principles

Employees must adhere to the following fundamental principles:

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

Access to the Thwaites 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 Thwaites IT systems.

**Individuals must not:**

• Allow anyone else to use their user ID/token and password on any Thwaites IT system.

• Leave their user accounts logged in at an unattended and unlocked computer.

• Use someone else’s user ID and password to access Thwaites IT systems.

• Leave their password unprotected (for example writing it down in a notepad /sticking it to a monitor or under a keyboard).

 • Perform any unauthorised changes to Thwaites 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-Thwaites authorised device to the Thwaites network or IT systems.

• Store Thwaites data on any non-authorised Thwaites equipment.

• Give or transfer Thwaites data or software to any person or organisation outside Thwaites organisation without the authority of Thwaites.

• Move any IT equipment such as PCs, printers, telephones, PDQs or tills without guidance from the IT Department

• Under any circumstances access the network cabinet or move any data cables without guidance from the IT Department

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 Thwaites 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 Thwaites in any way, not in breach of any term and condition of employment and does not place the individual or Thwaites 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 Thwaites 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 Thwaites, alter any information about it, or express any opinion about Thwaites, unless they are specifically authorised to do this.

• Send unprotected sensitive or confidential information externally.

• Forward Thwaites mail to personal non-Thwaites email accounts, for example a personal Gmail account.

• Make official commitments through the internet or email on behalf of Thwaites 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 Thwaites 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, Thwaites 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:

• 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.

Care must be taken using mobile devices in busy places in order to shield the screen from view of 3rd parties sitting in the near vicinity so as to prevent the screen being read.

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

**Individuals must not:**

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

**Viruses**

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

**Actions upon Termination of Contract**

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

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

**Monitoring and Filtering**

All data that is created and stored on Thwaites computers is the property of Thwaites and there is no official provision for individual data privacy, however wherever possible Thwaites 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. Thwaites 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 2018, 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, the IT department 01254 686860 or the Data Protection Officer.**

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

I confirm I have read and understood the above

Name …………………………………………………………………………….

Signed ……………………………………………………………………………. Date ………………………………………….