INTERIM

IT Acceptable Use Policy and Procedure

Version: 1.0	Date: March 2020	Owner:

Table of Contents

1 Statement of Purpose

As part of the current Covid-19 advice we have issued this temporary policy to help set out our IT Acceptable Use policy and approach.

This policy outlines the standards you must observe when using these systems, when and how we may monitor their use, and the action we will take if you contravene these standards.

2 Scope

This policy applies to employees, volunteers and contractors or consultants who need to use our IT systems to fulfil their contracted obligations, referred to within this Policy as 'Users'.

This policy and procedure does not form part of any terms and conditions of employment and it can be amended at any time.

3 General Principles

Our intention in publishing an Acceptable Use Policy is not to impose restrictions that are contrary to our desired culture of openness, trust and integrity. We are committed to protecting our employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowing whilst working from home during this crisis.

Breaches of this Policy will be investigated, and appropriate actions will be undertaken

4 User Responsibility

Access to our IT systems is controlled using User IDs, passwords and/or tokens. All information stored on electronic and computing devices whether owned or leased by us, the employee or a third party, remains the sole property of ourselves.

All Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information. Users may access, use or share proprietary information only to the extent it is authorised and necessary to fulfil their assigned job duties.

IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on our IT systems.

Users must not:

- Allow anyone else to use your userID/token and password on any of our IT systems
- Leave your user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access our IT systems.
- Leave your password unprotected (for example writing it down).
- Perform any unauthorised changes to our IT systems or information.
- Attempt to access data that you are not authorised to use or access.
- Connect any device not authorised by ourselves to any of our networks or IT systems.
- Store our data on any non-authorised equipment unless authorised
- Give or transfer our data or software to any person or organisation without the authority of ourselves.

5 Internet and Email Conditions of Use

Our internet and email are intended for business use. Some personal use is permitted, provided that work practices or security are not unduly affected. This right may be withdrawn if private usage is regarded as unreasonable in any individual case.

All Users are accountable for their actions on the internet and email systems. When using company resources to access and use the Internet, Users must recognise that they represent the company. Whenever employees state an affiliation to the company (including listing themselves as an employee of ourselves on their private social media profile), they must conduct all communications according to proper business etiquette, and also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Under no circumstances is a User authorised to engage in any activity that is illegal under UK or international law while utilising resources owned by ourselves.

The following activities are prohibited. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use:

System and Network Activities

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by ourselves.
- Unauthorized copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which or the end user does not have an active license.
- Accessing data, a server or an account for any purpose other than conducting business, even if you have authorized access to it.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a computing asset to actively engage in procuring or transmitting material of a sexual, degrading, offensive or otherwise illegal nature or any other material which violates UK or international law.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a User's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, employees to third parties
- Removing or disabling anti-virus software.
- Attempting to remove virus-infected files or clean up an infection, other than using approved anti-virus software and procedures that have been approved by ourselves

Email and Communication Activities (including Social Media and Blogging)

- Using profanity, obscenities, or derogatory remarks in communications.
- Accessing, downloading, sending or receiving any data (including images), which is offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Using the internet or email to make personal gains or conduct a personal business.
- Using the internet or email to gamble.
- Using the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or other electronic means, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within our networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by or connected via our network.
- Sending unprotected, sensitive, or confidential information, or any information which could jeopardise our intellectual property externally, including to your own personal email address.
- Downloading copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- Downloading any software from the internet or accept the terms and conditions of website agreements without prior approval of their Manager.
- Storing personal files such as music, video, photographs or games on our IT equipment.
- Placing any information on the Internet that relates to ourselves, alter any information about it, or express any opinion about ourselves, unless they are specifically authorised to do this.

6 Working at home

When working from home the following controls must be applied:

- Equipment and media must not be left unattended in public places and not left in sight in a car.
- 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.

7 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 mobile storage devices authorised by us must be used when transferring sensitive or confidential data.

8 Software

- Users must use only software that is authorised by ourselves on our computers.
- Authorised software must be used in accordance with the software supplier's licensing agreements.

9 Review

We will review and ensure compliance with this policy at regular intervals during this current crisis and will update you accordingly of any changes.