# COMPANY IT

**INTRODUCTION**

The purpose of [Insert Company Name] IT policy is to ensure business continuity and to minimise operational damage by reducing the opportunity for and impact of security threats and risks.

**SCOPE**

This policy applies to all users of our IT Systems, inclusive of employees, freelancers, contractors and any other third-party providers. This includes IT hardware, software, facilities and processes owned or otherwise made available by us or on our behalf.

You are expected to abide by this IT policy and failure to do so; or acts that constitute a breach; will be dealt with severely under the Company disciplinary rules up to and including summary dismissal for those employed, and may result in termination in contractual relationships for non-employees.

## AUTHORISED USE / ACCESS

You are reminded that any equipment, hardware or software provided by us for use in your work remains the property of the company including Internet, e-mail and social media facilities, as well as any data residing on our IT equipment. Access may be granted to you in support of your day-to-day work and you are expected to use your access to the IT resources efficiently and responsibly in support of this. Any access granted to you is on trust and must not be transferred or extended to any other individual or group, internally or externally, without prior approval of the manager responsible for IT in the company.

Please note that being granted access to our IT resources does not imply the right to use those resources. Consequently, we reserve the right to limit, restrict, remove or extend access to and privileges within, material posted on, or communications via its information technology resources, consistent with this policy, applicable law or as the result of company disciplinary processes, and irrespective of the originating access point.

## PASSWORDS

You are responsible for any activities carried out in respect of your password created under your own password and unauthorised and/or inappropriate use of a password will be treated as gross misconduct. If leaving a workstation unattended for any period of time, ensure it is logged off to prevent unauthorised users accessing it and keep your passwords confidential. All passwords should contain a mixture of alpha and numeric characters.

## AUDITING

We shall audit our IT resources in order to maintain accurate records of our hardware, software and system structure. Any changes to the IT resources must be approved in advance and fully documented, ensuring continuity of information, and therefore support, by all relevant members of the company. No changes should be made without prior authorisation.

## COMPUTER EQUIPMENT DISPOSAL

You must not dispose of any software or hardware owned by the company without authorisation.

**PROCUREMENT**

Unless authorised, you are not permitted to source and/or purchase any IT hardware, software and/or any associated peripherals or spares. If you purchase any of these without prior authorisation, you will not be reimbursed.

**NETWORK AND SYSTEM INTEGRITY**

Any behaviour and/or activities that threaten the integrity of our computer networks or systems are expressly prohibited and will be considered as acts of Gross Misconduct. Such behaviour and/or activities include but are not limited to;

* Interference/disruption of systems, networks or related services, including but not limited to the propagation of computer ‘worms,’ ‘viruses’ or ‘Trojan Horses’.
* Intentionally or carelessly performing an act that places an excessive load on a computer or network resulting in the disruption of our services.
* Failure to comply with requests to discontinue an activity that threatens the operation or integrity of computers, systems or networks.
* Negligently or intentionally revealing passwords or otherwise permitting the use by others of logon accounts for computer and network access.
* Altering or attempting to alter files or systems without authorisation.
* Unauthorised scanning of ports, computers and networks.
* Unauthorised attempts to circumvent the UK General Data Protection Regulations (UK GDPR) and the company’s data protection schemes, anti-virus software or to uncover vulnerabilities in the company’s security systems.
* Connecting unauthorised equipment to our network or computers.
* Attempting to alter any of our computing or network components without authorisation or beyond one's level of authorisation, including but not limited to bridges, routers, hubs, wiring, and connections.
* Utilising network or system identification numbers or names that are not assigned for one's specific use on the designated system.
* Using our resources to gain unauthorised access to any computer system and/or using someone else's computer without their permission.
* Providing services or accounts on our computers or via our networks to other users from a personal computer unless required to meet the normal activities of authorised business.
* Hosting an unauthorised web-site on any of our resources or registering a domain name on any company-owned or leased equipment or utilising any of the company’s IT resources for that purpose unless authorised to do so.
* The connection of ANY device whatsoever [or drivers for such a device] to the company’s IT resources without authorisation – this includes but is not limited to; printers, PDA’s, laptops, standalone or network desktop PC’s.

Authorisation to carry out any of the above must be sought in writing before such activity takes place.

**PERSONAL DATA**

The company understands its responsibility to protect personal data and any behaviour that breaches the company’s GDPR, Data Protection and IT Policies will be managed under the company’s disciplinary procedure and will be considered an act of Gross Misconduct and may result in your summary dismissal.

## MISUSE OF EQUIPMENT

Please note: if you misuse and/or abuse any telecommunications or electronic equipment or method of storing, transferring or transmitting data, this may result in appropriate disciplinary action being taken, which could include summary dismissal. In cases where you are a contractor or seconded from an agency, violation of this policy will result in contract termination and possible disciplinary action by their employer/service provider.

## DOWNLOADING OF FILES

You are expressly forbidden to download any applications, (including mobile apps), executable files (.exe, com or .bat extensions), or other files, games, apps, or screensavers, or to initiate any software upgrades from the Internet, cloud-based systems, e-mail, or via USB, CD-ROM/DVD or any other media to the organisation’s network system, or to an individual PC, unless specifically directed to do so by the manager responsible for IT in the company.

## BRING YOUR OWN DEVICE (BOYD)

Under some circumstances we may allow you to utilise a personally owned device to either connect to our IT infrastructure, or to receive, transfer or store company data such as emails, contacts or documentation. Permission must be sought from the person responsible for our IT and manager in the first instance and you MUST abide by this policy.  Any breach of this policy will be managed under our disciplinary procedure and will be considered an act of Gross Misconduct.

## UPLOADING OF FILES

## Except where we have granted permission to do so under a BOYD policy, the uploading of files and documents bellowing to the company to any cloud-based system outside of the company’s IT systems, via email, or onto any USB, CD-ROM/DVD or any other media, computer, phone, or other system, or to any other person except in the proper conduct of your duties, without the permission of the company is expressly forbidden.

## Upon leaving the company regardless of the reason, unless you have express written permission to retain any files or documents, you should delete anything that may be the property of the company as failure to do so may be regarded as theft of confidential and/or intellectual property. This may also be regarded as a breach of contract post-termination for which the company reserves the right to seek damages for such breach.

## MAILING LISTS AND NEWSGROUPS

Please take care when signing up to mailing lists or news groups as these sites can produce a lot of unnecessary traffic which may impact upon the effectiveness of the company’s IT systems. The manager responsible for IT in the company retains the right to delete any such access.

## ANTI-VIRUS

{Insert Company Name] is committed to maintaining its IT resources as “virus-free”, to ensure the efficient operation of our systems and will use up to date virus scanning software in this respect. To assist with this, you are requested to follow some basic rules;

* Ensure any transferable media is scanned before use on company systems.
* Do not download files from e-mail/Internet unless the source is verified virus-free.
* Ensure vendors run demonstrations on their own machines not the company’s.
* Inform the person responsible for IT immediately if virus infection is suspected.

We will ensure that;

* Only clean, original master copies of software shall be used when building systems.
* Any reports/cases of virus infection shall be fully investigated and eradicated as soon as practicable
* All users shall be informed of any issues or infections relating to virus contamination.

## MOBILE / LAPTOP/TABLET USERS

If you are granted the use of our mobile communication equipment, the above policies equally apply and additionally;

* Do not allow non-staff members to use the equipment.
* Do not store any personnel details on these computers.
* Ensure that Anti-virus software is installed and working on the equipment.
* Do not leave any equipment on view in a vehicle.
* Do not install any additional software on this equipment.
* Remember you are personally liable for any unlicensed software, and copyrighted material found on this equipment, and will be subject to the company’s disciplinary procedures for any breach of this policy.