Dated 12th March 2024

IT & DATA PROTECTION POLICY

SCOPE

References to the IT Department cover both the Company IT systems, and/or that of the Customer. Customer IT policies take precedence over this policy when operating equipment at the customer site, on equipment supplied by the customer. References to a ‘PC’ by extension to their similarity and functionality include all personal computers, laptops, tablet devices, mobile phone devices, external disk drives, memory sticks and other data storage devices.

Specific consideration has been given to the following sections of BS EN ISO 9001:2015:

1) 7.1.3 - Infrastructure

2) 8.1 – Operational Planning

PC USE

You should only use computer hardware and software supplied by the Company. Using other equipment or installing other programmes can lead to viruses being introduced into the Company network or that of the customer, and potentially breaching licence agreements. Unauthorised or unlicensed software must not be installed on Company or customer PCs. Nor should you under any circumstances copy or transfer licensed software without the prior express approval of the IT Department. If a virus is detected that can be traced back to unauthorised software being installed by an employee, this will be dealt with as a disciplinary matter. Using unlicensed software is a breach of any given software licence agreement and could result in the Company, customer and/or individual using it being fined by the software house if discovered. This would also be considered a disciplinary matter for the employee concerned. To protect yourself, do not allow non-authorised staff or subcontractors to use a PC or laptop designated for your use or under your control.

PREVENTING UNAUTHORISED ACCESS

All devices used to access any part of the Company network (including but not limited to the Email system and any Document storage of Sharing facilities) should display some form of access control in the preferred form of a password and/or PIN reference. This password or reference should be kept private and used expressly by the person to whom it belongs.

BACKING UP DATA

If you use a Company or customer PC on a regular basis it is imperative that you make sure that files and data are backed up regularly in the designated area (of the PC or on a separate

disk drive as advised to you by the customer or the Company, or on the Company Server). Should such a facility not be immediately available to you, please advise your Line Manager accordingly.

UNAUTHORISED ACCESS / COPYING OF DATA

You should only access the files, folders, directories and servers that you have authority to view. Unauthorised or attempted access to restricted areas will be dealt with as a disciplinary matter. You may not copy or remove from your place of work any files, disks, or USB Flash Drives or memory sticks without the permission of your manager.

PASSWORDS

You should keep your password safe and not reveal it to, or exchange it with anyone else, or use another employee's password to gain access to the system. If you do this, you could be held liable for loss of data, damage to the PC, downloading of inappropriate material from the internet or the sending of inappropriate emails, by someone else. This could lead to disciplinary action being taken against you.

INTERNET AND EMAIL

Under normal circumstances you are not permitted to send personal emails or view internet sites without the express prior permission in writing from the Company or the customer. If you are authorised to use the Internet, you should only do so in the course of your duties and be aware of potential risks to both you and the Company. If you are authorised to send emails on behalf of the Company, you should ensure that the content is both professional, polite, and relevant to the intended recipient.

It is essential that you do not open or download email attachments from unknown sources as they may contain viruses that can damage the PC or IT network. Attachments which may contain viruses can include 'doc' files, 'zip' files and other non descript files. If in doubt, query the email content with your Line Manager who will escalate the query accordingly.

Company emails should include a brief signature to assist in your identification to the intended recipient, and this should include your name, title, contact telephone number and where possible with email software, a graphical image displaying the Company accreditations.

MONITORING

You should be aware that the Company reserves the right to monitor e-mails, internet use, location, faxes and telephone calls in certain circumstances, in order to protect its business interests, and in accordance with current legislation. This includes personal and business communications. In doing so the Company will observe the good practice recommendations set out in the Information Commissioner's Employment Practices Code, Part 3, which deals with monitoring and surveillance and these may include providing evidence of a commercial transaction, providing evidence of other business communications to establish facts, or ascertain compliance, with regulatory practices or procedures, audit, debt recovery, dispute resolution, preventing or detecting crime, detecting the unauthorised use of the electronic communications system, protecting against viruses or hackers and combating or investigating fraud or corruption. The Company also reserves the right to access your email account in the event that you are on annual leave, extended leave, sickness leave, or in any event where failure to do so may not be in the Company's interests.

BREACH OF IT POLICY

Failure to comply with the IT Policy and, in particular the guidelines for acceptable use of e-mail and the Internet may be addressed via the Company's disciplinary procedure and depending on the seriousness of the breach, could lead to disciplinary action being taken against you up to and including dismissal. If you are uncertain about any aspect of this policy, please speak to your manager.

DATA PROTECTION POLICY

As part of running a business, the Company needs to collect and use personal data about people including past, present and prospective employees as well as customers and suppliers. Any personal data we collect, record or use in any way, whether it is held on paper, on computer or other media will have safeguards applied to it to make sure we comply with the Data Protection Act 1998 ("the Act").

In order to meet the requirements of the Act we will:

- Observe the conditions regarding the fair and lawful collection and use of personal data, including the conditions set out for collecting general data and sensitive personal data in Schedule 2 and Schedule 3 to the Act respectively;
- Meet our obligations to specify the purposes for which data is used;
- Collect and process appropriate personal data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of personal data used;

- Apply strict checks to determine the length of time personal data is held;
- Ensure that the rights of individuals about whom the personal data is held can be fully exercised under the Act;
- Take appropriate security measures to safeguard personal data; and
- Ensure that personal data is not transferred abroad without suitable safeguards.

When we collect any personal data from you we will inform you why we are collecting your data and what we intend to use it for. Where we collect any sensitive data, we will take appropriate steps to ensure that we have explicit consent to hold, use and retain the information. Sensitive data is personal data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.

Your rights include the right to:

- Request a copy of the information held about you
- Request inaccurate information about you to be corrected
- Prevent processing likely to cause damage or distress
- Prevent processing for the purposes of direct marketing
- Seek compensation if you suffer damage/distress as a result of a breach of the Act by the Company.

If you have any queries about your rights in this area or would like a copy of the personal data stored on you which is covered under the Act, please discuss this with your manager or supervisor who will contact the Data Protection Officer. There will be a maximum fee of £10 for access to your records which must be provided to you within 40 days of receipt of your request and your cheque, subject to certain criteria involving the confidentiality of third parties, and you satisfactorily verifying your identity. If you have any complaints about the Company response to your requests, this should be taken up via your manager through the Grievance procedure. If you are involved with the keeping of information, either manually or on a computer, about either staff or other individuals, you have an obligation to see that it is accurate, factual and not flippant and not passed on in any unauthorised way. This means that all information is confidential and you should not discuss the details with anyone other than those authorised to have that information. If you are found to have permitted unauthorised disclosure, you will be subject to disciplinary action up to and including dismissal.

In operating CCTV, the Company will observe the good practice recommendations set out in the Information Commissioner's Code of Practice, which deals with monitoring and surveillance. The name of the current Data Protection Officer for the Company can be obtained from your manager. The Data Controller is the Company itself.