Data Protection Policy

Compliance with Data Protection Regulations:

To ensure we are in compliance with Data Protection Regulations, including General Data Protection Regulation (GDPR), the Company has taken various measures to ensure we are meeting all requirements, as follows:

- **Data Protection Officer** – our management system identifies key responsibilities including details of our Data Protection Officer (DPO)
- **Personal Data collected** – we do not actively collect or process any personal information other than the details of our employees'. We may also hold some personal data from interactions with prospective and existing customers and systems are in place to manage such data.
- **Sensitive Personal Data** – we do not collect or hold any sensitive personal data. Should you believe this not to be the case, the DPO should be advised accordingly
- **Data retention** – data retention is managed and retention periods are documented in our management system manual
- **Consent** – if any data is to be collected for any purpose other than normal employment purposes, we will obtain your explicit consent and you have the right to withdraw this consent at any time
- **Privacy by Design** – any new developments, projects or technologies that involve personal data will be reviewed, to ensure privacy by design and a privacy impact assessment completed
- **Data Processing/Transfer** – personal data is processed and handled in a lawful and transparent manner, with clear communication of what data we hold, why we hold it and how long we will retain it. We will not transfer personal data to any third party except to those approved for the purposes of ongoing personnel and payroll administration
- **International Transfer of Data** – we do not envisage transferring your personal data outside of the European Economic Area (EEA) or to any international organisation, however if we do, it will only be to comply with our legal or contractual requirements and we will inform data subjects in any event of international transfer
- **Data Subject Access** – data subjects have the right to access, correct, transfer or request deletion of the personal data we hold about them. Subject Access Requests (SAR) should be directed to our DPO who will respond to all such requests within one (1) month. We will not charge for responding to such requests
- **Data Security** – we have measures in place to protect Confidentiality, Integrity and Accessibility of all Company data
- **Data Breaches** – all data breaches will be reported internally and significant breaches will be reported to the Information Commissioner's Office (ICO). Affected data subjects will be notified within seventy-two (72) hours of discovery of said breach

Much of the arrangements for management of data, documented information, ongoing checks including internal audits, are all covered by our ISO9001 compliant integrated management system which is available to all staff.

Protection of Personal Data

Care must be taken to ensure all staff comply with Data Protection Regulations. All staff must ensure personal data is controlled and secure and details are not disclosed to any other person (whether inside or outside the Company) unless authorised to do so. All staff are made aware of Data Protection and Information Security obligations and are also made aware of this Policy, our Privacy Policy and any other relevant Company Policies.

Failure to comply with any of the requirements of this Policy is a contravention of our Company's standards of behaviour and is a disciplinary offence, which may result in disciplinary action being taken against you in accordance with our Company's disciplinary procedure.

Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

Signed:

Lynn Wilson
Data Protection Officer
28th February 2023