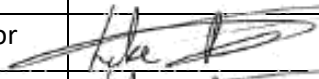
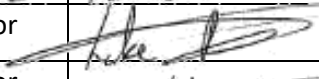
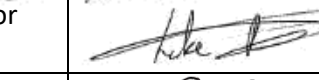
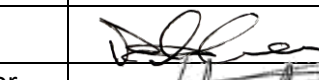


DATA PROTECTION

DOCUMENT TITLE: Data Protection

REVISION: 1.01

DOCUMENT CONTROL LOG:

	Name	Role	Signature	Date	Rev
Prepared By	Luke Deasy	Managing Director		10/02/2023	1.01
Reviewed By	Luke Deasy	Managing Director		12/06/2023	1.01
Reviewed By	Luke Deasy	Managing Director		12/06/2024	1.01
Reviewed By	Peter Lane	EHS Officer		12/06/2025	1.01
Reviewed By	Luke Deasy	Managing Director		12/06/2026	1.01

DATA PROTECTION POLICY:

The Data Protection Policy is a statement of the Company's commitment to protect the rights and privacy of individuals with whom we come into contact during the course of our work in accordance with the General Data Protection Regulations and Data Protection Act 2018 (as amended). All employees are obligated to always handle personal data with confidentiality. Data protection laws safeguard the privacy rights of individuals in relation to the processing of their personal data. This includes personal data of employees and clients. We refer you to the Company's GDPR Policy and Privacy Policy for further information.

The Company has overall responsibility for ensuring compliance with the data protection legislation, including the Data Protection Act 2018 (as amended), when it is the Data Controller of personal data (as defined in the Data Protection Act). However, all employees of the Company that separately collect and/or control the content and use of personal data are individually responsible for compliance with all data protection legislation.

In compliance with the GDPR and data protection legislation, the Company shall take measures to guard against unauthorized access to computer based personal data and against its alteration, disclosure or destruction. It is the responsibility of each device (for example laptop, PC, tablet, mobile phone, etc.) owner to ensure that the device is appropriately secure.

Any violation of data protection laws in relation to the Company, its business, its employees, clients, suppliers or other persons with whom the company does business is required to be reported to the employee's direct Manager immediately.

Any misuse or abuse of personal information, passwords and or access to the Company's information systems is subject to review through the Company's Disciplinary Procedure and appropriate action may be taken in line with this procedure up to and including dismissal.

The Right to Access is an important right for individuals (employees and residents), allowing them to obtain information about the kinds of data the Company processes about them, and to verify that the information is accurate and up to date. A data subject who wishes to gain access to information about them that has been collected, stored and used by the Company is required to make this request in writing to the employee's direct Manager.



Luke Deasy
Managing Director