USE OF OWN IT EQUIPMENT POLICY

1. Purpose

The purpose of this Policy is to establish clear requirements for the use of personal information technology ("IT") equipment by individuals engaged by the Company. It is designed to ensure that all Company data, systems and communications are protected against unauthorised access, misuse, or loss, whilst allowing flexibility for individuals to work remotely using their own devices.

2. Scope

This Policy applies to:

- All employees who use their own IT equipment to carry out Company duties from home.

3. Company Responsibilities

The Company will:

- Provide guidance on minimum IT security standards.
- Issue secure access credentials where necessary.
- Monitor compliance with this Policy in line with data protection and information security obligations.

The Company is not responsible for the procurement, maintenance, repair, or replacement of personal IT equipment.

4. Individual Responsibilities

All individuals using their own IT equipment for Company purposes are required to:

- Ensure their equipment is maintained in good working order and capable of meeting Company requirements.
- Keep operating systems, browsers, and software up to date with current security patches.
- Install and maintain reputable anti-virus/anti-malware protection.
- Protect their device with strong passwords and enable automatic locking when unattended.
- Use only secure, encrypted Wi-Fi connections (minimum WPA2 or equivalent).

5. Acceptable Use and Restrictions

- Personal devices may be used for any lawful personal purposes. However, when being used for Company business, individuals must follow this Policy and ensure that Company data is kept separate and secure.
- Company data must not be permanently stored on personal devices unless explicitly authorised.
- Company data may not be copied, transferred, or backed up to unapproved personal cloud services, external hard drives, or removable media.
- Employees must log out of company systems on personal devices when not actively in use.

6. Data Protection and Confidentiality

- All individuals must comply fully with the Company's Data Protection, Confidentiality, and Information Security Policies.
- Any suspected or actual data breach, loss of equipment, or unauthorised access must be reported to the Company immediately.
- Individuals acknowledge that failure to uphold these obligations may place the Company in breach of its legal obligations under data protection legislation.

7. Zero-Hours Employees

- All zero-hours employees must use their own IT equipment when performing services for the Company.
- Employees must ensure compliance with this Policy at all times.
- Failure to comply may result in immediate termination of the working arrangement and potential legal liability for any losses caused.

8. Monitoring and Enforcement

The Company reserves the right to:

- Audit compliance with this Policy.
- Require written confirmation from individuals that their personal IT equipment meets the required security standards.
- Take appropriate action, up to and including termination of employment or contract, in cases of breach.

9. Acknowledgement

All employees and contractors using personal IT equipment for Company purposes are required to confirm in writing that they have read, understood, and agree to comply with this Policy.
