Cyber Security Policy

Introduced: August 2025

Next review date: August 2026

Policy Statement

We Are Ease Limited is committed to protecting its information, systems, staff, customers, and suppliers from cyber threats. Our aim is to ensure that all company data and technology are safeguarded against unauthorised access, misuse, loss, or damage, and that everyone understands their role in maintaining a secure digital environment.

We value confidentiality, integrity, and availability of our information. Cyber security is the responsibility of everyone at We Are Ease Limited, and all staff are required to follow this policy to protect both company and client information.

1. Aims of the Policy

We will ensure that we:

- Protect company, staff, and client information against unauthorised access, disclosure, alteration, or destruction.
- Maintain compliance with relevant data protection and cyber security legislation (including GDPR and UK Data Protection Act 2018).
- Provide appropriate training and awareness to all team members.
- Establish clear roles and responsibilities for information security.
- Promote a culture where cyber security is embedded in everyday work practices.

2. Area of Responsibility

All individuals are responsible for:

- Using company systems, email, and devices responsibly and securely.
- Protecting passwords, devices, and data from misuse.
- Reporting suspected cyber threats, phishing attempts, or data breaches immediately.
- Following company procedures for data handling, storage, and communication.

Management is responsible for ensuring that:

- Appropriate security controls, software, and monitoring tools are in place.
- Access to sensitive data is restricted on a “need-to-know” basis.
- Regular backups and system updates are carried out.
- Staff receive ongoing cyber security training.

The enforcement of this policy is ultimately the responsibility of the Managing Director, and the content shall be reviewed on an annual basis.

3. Specific Cyber Security Requirements

3.1 Email Security

- Company email accounts must only be used for legitimate business purposes.
- Staff must not open suspicious attachments or click on unknown links.
- Emails containing sensitive information must be encrypted or password-protected where appropriate.
- Phishing or suspicious emails must be reported immediately.

3.2 Password Requirements

- Passwords must include a mix of letters, numbers, and symbols.
- Passwords must not be shared or written down in an insecure location.
- Multi-factor authentication (MFA) must be used wherever possible.
- Passwords must be changed immediately if a breach is suspected.

3.3 Remote Working

- Staff working remotely must connect via secure internet connections (not public Wi-Fi unless using a company-approved VPN).
- Company laptops, phones, and other devices must be encrypted and protected with strong passwords.
- Confidential conversations or document reviews should not take place in public spaces where information could be overheard or seen.
- Data must not be stored on personal devices or external drives without approval.

3.4 Use of Personal Devices

- Personal devices may only be used for work purposes with prior approval.
- Approved devices must have up-to-date security software and be password-protected.
- Company data stored on personal devices must be deleted when no longer required or when employment ends.
- Lost or stolen devices containing company data must be reported immediately.

3.5 Software & Updates

- Only authorised software may be installed on company devices.
- Devices must be kept up to date with security patches and antivirus software.
- Staff must not disable security features such as firewalls, encryption, or antivirus protection.

3.6 Data Protection & Storage

- Confidential information must be stored on secure company systems, not personal storage solutions (e.g., personal Google Drive, Dropbox).
- Data must only be accessed by authorised personnel.
- Any suspected data breach must be reported immediately.

4. Breach of Policy

Any breach of this policy, whether deliberate or accidental, may result in disciplinary action under the company's procedures. In cases where laws are broken, the company may notify the appropriate authorities.
If you suspect a cyber incident or security breach, you must report it immediately to your Associate Director or the Managing Director.

Signed  Date: 29th August 2025

Dafydd Hollyman, We Are Ease Ltd. Managing Director

Document Control

Version	Issue Date	Revision Date	Changes Made	Approved by:
1.0	29/08/2025	N/A	Initial Issue	D Hollyman (MD)