



## IT & Cyber Security Policy

### Purpose

To protect Everyday English Ltd's IT systems, networks, and data from unauthorised access, loss, or damage.

### Policy Statement

Everyday English Ltd will maintain secure and reliable systems, implement safeguards to prevent cyber threats, and respond effectively to any incidents.

### Legal Framework

- Data Protection Act 2018 (security obligations)
- UK GDPR (Article 32 – Security of Processing)
- NCSC Cyber Essentials guidance

### We will:


- Require all devices used for work purposes to be password-protected and, where possible, encrypted.
- Use multi-factor authentication for email and critical systems.
- Keep antivirus and firewall protection up to date.
- Back up important data regularly and store securely (offsite or in encrypted cloud storage).
- Prohibit the use of unauthorised software or hardware.
- Provide staff and volunteers with guidance on recognising phishing and other cyber threats.
- Report any suspected security incident to the IT Lead immediately.

### Breach of Policy

Failure to follow IT security procedures may result in disciplinary action and, where appropriate, legal action.

### Review

This policy will be reviewed annually by the Board of Directors.

Signed: 

Chair, Board of Directors

Date: 30<sup>th</sup> September 2025