

Data Protection and Information Security Policy

Introduction

At Jenny Garrett Global (Reflexion Associates Limited), we take data protection and information security seriously. This policy sets out our internal procedures and the technical measures we have in place to protect information.

We comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Responsibilities

Data Protection Representative: Tania Christopher is responsible for data protection compliance.

Everyone: All employees and associates are responsible for following this policy and reporting any concerns.

Security Measures

Certification

We hold Cyber Essentials certification, demonstrating our commitment to protecting against common cyber threats.

Access Controls

- Access to systems and data is restricted to authorised personnel only
- We use role-based access controls
- Access rights are reviewed regularly and removed when no longer needed

Passwords and Authentication

- Passwords must be at least 12 characters, using a mix of characters
- Two-factor authentication is required for key systems
- Password managers are encouraged

Encryption

- Our website uses SSL/TLS encryption (HTTPS)
- Data is encrypted in transit and at rest where appropriate
- Laptops and devices are password-protected

Backups

- Regular automated backups of key data
- Backups are stored securely and tested periodically

Software and Updates

- Security updates are installed promptly
- Anti-virus software is used and kept up to date
- Only authorised software is installed on work devices

Data Handling

- Personal data is only collected when necessary and with appropriate consent or legal basis
- Data is stored in secure, UK-based systems
- Data is retained only as long as needed and then securely deleted
- Confidential information is not sent via unencrypted email where avoidable

Remote Working

Many of our team work remotely. The same security standards apply regardless of location:

- Work is only done on approved, secure devices
- Public Wi-Fi is avoided for sensitive work
- Screens are locked when unattended
- Confidential conversations are held privately

Data Breaches

If you suspect a data breach or security incident, report it immediately to Tania Christopher. We will:

- Investigate and contain the breach
- Assess the risk to individuals
- Report to the ICO within 72 hours if required
- Notify affected individuals where necessary
- Learn from the incident and improve our processes

Training

Everyone who handles data receives appropriate training on data protection and information security.

ICO Registration

We're registered with the Information Commissioner's Office. Registration number: ZA454896

Signed: Jenny Garrett OBE

Date: December 2025

Next review: December 2026