

Data Security Policy

Centre Name: 4 TEFL

Responsible Person: Ruswel James, Quality Assurance

Review Date: 30 September 2025

1. Purpose

The purpose of this policy is to ensure that all learner and staff data at 4 TEFL is collected, stored, processed, and protected securely. This supports compliance with the UK GDPR, the Data Protection Act 2018, Ofqual regulations, and Focus Awards requirements.

2. Scope

This policy applies to:

- All personal data of learners, staff, assessors, and stakeholders.
- All systems used by 4 TEFL, including the CRM, e-learning platform, Zoom sessions, and cloud servers in the UK, EU, and Canada.
- All staff, contractors, and service providers handling data on behalf of 4 TEFL.

3. Roles and Responsibilities within 4 TEFL

- **Quality Assurance (Ruswel James):** Data Protection Lead, responsible for implementing this policy and liaising with the ICO.
- **Assessors/IQAs:** ensure assessment and learner records are stored securely and only shared when necessary.
- **Administrative staff:** maintain secure handling of registration and certification data.
- **Learners:** expected to use strong passwords and keep login details confidential.

4. Data Security Principles

- **Confidentiality** – Data is only accessible to authorised staff.
- **Integrity** – Data is accurate and kept up to date.
- **Availability** – Data is accessible for legitimate use when required.
- **Minimisation** – Only necessary data is collected and processed.
- **Accountability** – All staff are trained and accountable for data protection.

5. Technical and Organisational Measures

- Data stored on secure servers in the EU and Canada with encryption in transit and at rest.
- Identity verification for regulated courses is conducted via **Stripe Identity** with minimal data retention.
- Access to CRM and e-learning platform restricted by role-based permissions.
- Regular system monitoring, penetration testing, and backups.
- Staff training on phishing awareness, password security, and GDPR compliance.

6. Data Breach Procedure

1. **Identification** – Any suspected breach must be reported immediately to the QA.
2. **Containment** – Systems are secured to prevent further access.
3. **Assessment** – The QA investigates the scope and impact of the breach.
4. **Notification** – If required, the ICO and affected individuals will be informed within 72 hours.
5. **Remediation** – Corrective actions and preventive measures are documented.

7. Related Policies

- [Data Protection and GDPR Policy](#)
- Data Retention Schedule
- Privacy Policy
- Safeguarding Policy

8. Monitoring and Review

- Data security incidents and risks are logged in the CRM.
- Policy effectiveness is reviewed annually or following a breach.
- Updates are made in line with ICO guidance, Ofqual regulations, and Focus Awards requirements.

This policy has been approved & authorised by:

James Ruswel
Quality Assurance
30 September 2025

