

Security Procedures 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 4 TEFL maintains secure systems, environments, and practices to protect learners, staff, assessment integrity, and organisational assets. Security covers both physical and digital measures, aligned with Ofqual and Focus Awards requirements.

2. Scope

This policy applies to:

- All learners, staff, assessors, IQAs, and contractors.
- All systems and environments used by 4 TEFL, including CRM, e-learning platform, Zoom, cloud servers, and internal communication systems.
- All assessment and certification processes.

3. Roles and Responsibilities within 4 TEFL

- **Quality Assurance (Ruswel James):** responsible for implementing, monitoring, and reviewing security procedures.
- **IT and development team:** ensure secure server management, encryption, monitoring, and backups.
- **Assessors/IQAs:** protect learner evidence and maintain secure assessment practices.
- **Administrative staff:** secure handling of learner records and certification processes.
- **Learners:** required to keep login credentials confidential and follow platform security guidelines.

4. Physical Security

- Office-based staff (where applicable) must ensure secure storage of any physical learner records.
- Visitors must be authorised and supervised.
- Equipment must be stored securely when not in use.

5. Digital Security

- CRM, e-learning, and Zoom systems are protected with encryption and role-based access.
- Servers are located in the EU and Canada, with secure backups and monitoring.
- Identity verification is conducted via **Stripe Identity** for Ofqual-regulated qualifications.
- Two-factor authentication is used for staff accounts accessing sensitive data.
- Regular penetration testing and security audits are conducted.

6. Assessment Security

- All assessments are stored securely in the CRM system.
- Zoom sessions are recorded and stored as part of evidence.
- Access to assessment materials is restricted to authorised staff only.
- Suspected breaches are reported immediately under the Malpractice and Maladministration Policy.

7. Incident Management

- All security incidents must be reported immediately to the Quality Assurance.
- The QA will investigate, record findings, and take corrective actions.
- Serious incidents involving data breaches will follow the [Data Security Policy](#) and ICO reporting requirements.

8. Monitoring and Review

- Security procedures are monitored continuously by the QA and IT team.
- Regular reviews are conducted to identify risks and improve processes.
- This policy is reviewed annually or sooner if new risks emerge or regulatory requirements change.

This policy has been approved & authorised by:

James Ruswel
Quality Assurance
30 September 2025

