

Data Protection and GDPR Policy

Centre Name: 4 TEFL

Responsible Person: Ruswel James, Quality Assurance

Review Date: 30 September 2025

1. Policy Statement

4 TEFL is committed to protecting the privacy and security of all personal data processed in the course of its activities. This policy sets out how we comply with the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). It applies to all staff, learners, and stakeholders associated with 4 TEFL.

2. Principles of Data Protection

4 TEFL adheres to the following principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

3. Responsibilities

- The Quality Assurance (Ruswel James) is the Data Controller with overall responsibility for compliance.
- All staff members are responsible for following this policy and ensuring safe handling of personal data.
- Learners are expected to provide accurate information and respect confidentiality requirements.

4. Data Collected and Processed

Personal data collected may include names, contact details, identification documents, assessment records, lesson recordings, and CPD logs. Data is collected only for legitimate educational and regulatory purposes.

5. Security of Data

All data is stored securely on encrypted servers located in Europe and Canada. Access is restricted to authorised staff via secure login credentials. All Zoom sessions and assessment evidence are stored within the CRM system with controlled access.

6. Data Retention

Data will be retained in accordance with the 4 TEFL Data Retention Schedule. After the retention period expires, data will be securely deleted or anonymised.

7. Learner Rights

Under the UK GDPR, learners have the right to:

- Be informed about data collection and processing.
- Access their personal data.
- Rectify inaccuracies.
- Request erasure ('right to be forgotten').
- Restrict or object to processing.
- Data portability.

8. Data Breach Procedure

Any data breach will be reported immediately to the Head of Centre. Serious breaches will be notified to the Information Commissioner's Office (ICO) within 72 hours, in line with legal obligations.

9. Related Policies

This policy should be read in conjunction with:

- [Identity Verification Policy](#)
- [Complaints Policy](#)
- [Appeals Policy](#)

10. Monitoring and Review

This policy will be reviewed annually or earlier if legislation changes. Compliance will be monitored by the Head of Centre and IQA as part of Quality Assurance processes.

This policy has been approved & authorised by:

James Ruswel
Quality Assurance
30 September 2025

