GDPR Policy

Scope and Context

This policy outlines how Tyneside Training Services collects, processes, stores, and protects personal data in compliance with the UK GDPR, Data Protection Act 2018, and the Data (Use and Access) Act 2025. It applies to all personal data handled while delivering logistics training and apprenticeships, including data related to learners, employers, staff, subcontractors, awarding bodies, and funding agencies.

This policy applies to all employees, contractors, and stakeholders of Tyneside Training Services who handle personal data in the course of their duties. It covers all personal data processed by the organisation, whether held digitally or in physical form, and applies to all training, administrative, and operational activities.

This policy supports our accountability obligations and ensures that personal data is handled lawfully, fairly, and transparently as stated within the seven core principles of the GDPR.

TTS complies with the following legislation:
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Data (Use and Access) Act 2025 (DUAA)

Commitment Statement

Tyneside Training Services is committed to:

- Upholding the six principles of data processing: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.
- Respecting the rights of data subjects, including access, rectification, erasure, and objection.
- Implementing appropriate technical and organisational measures to safeguard data.
- Ensuring that all staff receive regular training and understand their responsibilities.

1. Data Protection

TTS processes personal data lawfully, fairly, and transparently. We ensure that data is collected for specified, explicit, and legitimate purposes and is not further processed in a manner incompatible with those purposes. We maintain data accuracy and limit storage to what is necessary.

2. Data Collection and Use

TTS collects personal data for:
- Course registration and delivery
- Certification and accreditation
- Employment and HR purposes
- Health and safety compliance
- Reporting to public sector funders such as the Department for Education (DfE) Combined Authorities, and the Education and Skills Funding Agency (ESFA)
- Marketing (with consent)

3. Data Sharing

TTS may share data with:
- Awarding Organisations
- Public sector funders and regulatory authorities such as Dfe, NECA and ESFA
- IT service providers
- Legal and professional advisors
- Employers (if training is employer funded)

All third parties are contractually bound to comply with GDPR and the Data (Use and Access) Act 2025.

4. Data Subject Rights

TTS recognises and upholds the rights of individuals, including:
- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making

5. Retention and Disposal of Data

TTS maintains accurate and up-to-date records in accordance with statutory and operational requirements. All learner records are retained for 6 years post completion of programme. Financial records are maintained for 6 years from the end of the financial year. Health & Safety Records are kept for a minimum of 3 years, or guided by the Health and Safety Executive (HSE) and relevant laws.

Access to records is controlled and monitored to ensure confidentiality and integrity.

Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the 'rights and freedoms' of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

6. Information Security

TTS implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This includes access controls, encryption, secure storage, and regular security audits. Staff are trained in information security best practices.

7. Operational Procedures and Guidance

To support the implementation of this policy, TTS provides operational procedures and guidance documents. These resources are readily available to all staff and are designed to ensure consistent and compliant handling of personal data. They provide clear instructions on data handling, breach reporting, and data subject rights.

8. Roles and Responsibilities

TTS is a data controller under the GDPR.
Managers, and all those in managerial or supervisory roles throughout TTS are responsible for developing and encouraging good information handling practices within TTS.
Roles and responsibilities for data protection, records management, and information security are clearly defined. The Data Protection Officer (DPO) oversees compliance and provides guidance. Managers are responsible for ensuring their teams adhere to policies and procedures.

The DPO has been allocated responsibility for TTS's compliance with this policy on a day-to-day basis and has direct responsibility for ensuring that TTS complies with GDPR, as do Managers in respect of data processing that take place within their area of responsibility. They will also act as a first point of call for staff seeking clarification on any aspect of data protection clarification.
Compliance with data protection legislation is the responsibility of all employees/staff of TTS who process personal data.
Staff must not disclose personal data, without authorisation, or in line with TTS policy.
All staff have a duty to make sure they comply with the data protection principles. Staff must ensure that records are accurate, up to date, fair, kept and disposed of safely and in accordance with TTS policies.
Personal data whether electronic or paper based, should be stored securely. Information should only be removed from it's storage location when operationally necessary and with appropriate security measures in place.
All staff are responsible for completing mandatory training at a minimum of every 2 years. Training records are maintained and monitored.

Definition of a Data Breach

A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples include:

- Loss or theft of devices containing personal data
- Unauthorised access to systems
- Accidental sending of personal data to the wrong recipient
- Cyberattacks or malware infections

Breach Response Steps

Step 1: Identification and Reporting

- Any staff member who becomes aware of a breach must report it **immediately** to the DPO.

Step 2: Containment and Recovery

- Take immediate steps to contain the breach (e.g., disconnect affected systems, retrieve misdirected emails).
- Recover lost data where possible and prevent further unauthorised access.

Step 3: Risk Assessment

- Assess the nature, sensitivity, and volume of data involved.
- Determine the potential impact on individuals and the organisation.
- Evaluate whether the breach is likely to result in a risk to individuals' rights and freedoms.

Step 4: Notification

- If the breach poses a risk to individuals, notify the **Information Commissioner's Office (ICO)** within **72 hours**.
- If there is a high risk to individuals, notify the affected individuals without undue delay.
- Document all decisions and justifications.

Step 5: Investigation and Documentation

- Conduct a full investigation to determine the cause and scope.
- Record all findings, actions taken, and lessons learned.
- Maintain a **Data Breach Register** for all incidents, regardless of severity.

Step 6: Review and Preventative Action

- Review policies, procedures, and training in light of the breach.
- Implement corrective actions to prevent recurrence.
- Update risk assessments and security measures as needed.

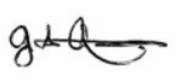
Contravention of this Policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under TTS disciplinary procedure which can be located within the staff handbook.

Policy Review

This policy shall be updated on an annual basis as a minimum but also in accordance with legislation or process changes.

Reviewed by: John Jones
Reviewer's position: Managing Director

Reviewer's signature: 

Review date: 15th July 2025
Next review date: 14th July 2026