TRS TRAINING LTD

Document title:	Data Protection and UK GDPR Policy	**Date of Issue:**	10/08/2026	**Date for review**	10/08/2027
Owner:	Beverley Ellis	**Issue Number:**	26-1	**Previous Version:**	25-1

This policy has been reviewed and approved by the Operations Director:	 Beverley Ellis

1. Policy Statement

TRS Training Limited is committed to full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We treat all personal data respectfully, lawfully and transparently, applying a duty of confidence and ensuring that data protection principles are embedded in our daily operations.

2. Scope of Policy

2.1. This policy applies to all TRS Training Limited's data processing and data-controlling activities, including personal data relating to applicants, learners, clients, employees, employers, suppliers, partners and any other individuals whose data we process.

2.2. All partners and third parties working with or for TRS Training Limited who may access personal data must read, understand and comply with this policy and with any Data Sharing Agreements (DSAs) or contractual data-processing clauses.

2.3. This policy does not apply when dealing with safeguarding concerns or referrals to the Disclosure and Barring Service (DBS). In such cases, TRS acts in accordance with Keeping Children Safe in Education (KCSIE) 2024 and statutory safeguarding guidance.

3. TRS Values

This policy underpins our commitment to our values, with particular reference to:

- RESPECT – All individuals and their unique talents
- RESPOND – Listening to our customers, partners and stakeholders and being equipped to meet their changing needs
- PARTNERS – Developing sustainable partnerships where everyone involved benefits from the relationship
- QUALITY – Providing outstanding teaching, learning and customer service

4. Implementation Principles

4.1. TRS Training Limited is both a **data controller** and **data processor** under UK GDPR.

4.2. TRS processes and controls personal data in accordance with UK GDPR principles, ensuring information is:

- used fairly, lawfully and transparently
- processed for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- retained only for as long as necessary
- protected through appropriate technical and organisational security measures

4.3. Data subjects may make Data Subject Access Requests (DSARs) as described in the Subject Access Request Procedure (Appendix 2). Data subjects have the right to:

- be informed
- access their personal data
- rectification
- erasure (where applicable)
- restrict processing
- data portability
- object to processing
- object to automated decision-making and profiling

4.4. The Data Privacy Notice (Appendix 1) explains what data TRS collects, how it is used, and the lawful bases for processing.

4.5. Data subjects may complain about any aspect of TRS's data processing. Complaints are handled in line with the Comments, Compliments and Complaints Procedure.

4.6. TRS conducts Data Protection Impact Assessments (DPIAs) where new technologies or processing activities may pose high risk to individuals' rights and freedoms. DPIAs cover digital systems including PICS, OneFile, SharePoint, employer systems used by learners, and any AI-enabled tools.

4.7. Where a DPIA identifies high risk that cannot be mitigated, the matter is escalated to the Board and may be referred to the ICO. Processing may only proceed once risks are reduced to an acceptable level.

Personnel Records

4.8. Employees must provide TRS with accurate personal details including home address, contact numbers, next of kin and bank details.

4.9. Employees must notify TRS immediately of changes to:

- name
- address or telephone number
- dependants
- beneficiaries
- emergency contacts
- bank details
- tax code

4.10. Employee records are stored digitally in secure systems. Employees may request access to their personal data, including a description of the purposes for which TRS processes it and who it may be disclosed to.

Disclosure of Data

4.11. TRS does not disclose personal data to unauthorised third parties. This includes family members, friends, government bodies and, in certain circumstances, the Police. Disclosure is only permitted when:

- authorised by TRS
- necessary for legitimate business purposes
- required by law
- related to safeguarding concerns

Consent

4.12. TRS understands consent to mean a freely given, specific, informed and unambiguous indication of the data subject's wishes. Consent may be withdrawn at any time by contacting info@trstraining.net.

4.13. Consent must never be obtained under pressure or through misleading information.

4.14. Applicants and clients may opt out of marketing at any time. Their choices must be respected.

4.15. Lead-generation campaigns must clearly state what data is collected, how it is used, retention periods and opt-out options.

4.16. Learners provide consent at enrolment for specific processing activities. Employers agree to data processing through the Contract for Services.

4.17. Explicit consent is required for processing special category data unless another lawful basis applies (e.g., safeguarding, legal obligation).

4.18. We use personal data collected on the TRS website only where we have received explicit permission or consent. Data collected on the website is managed in line with this Data Protection and UK GDPR Policy.

Security of Data

4.19. All staff must ensure personal data is kept secure and not disclosed to unauthorised parties.

4.20. Access to personal data is restricted and controlled through:

- Multi-Factor Authentication (MFA)
- role-based access controls
- digital audit trails
- secure cloud storage (PICS, OneFile, SharePoint)
- encryption at rest and in transit
- zero-trust access principles

4.21. TRS prohibits the use of removable media (USBs, external drives) for storing personal data.

4.22. TRS is a fully digital provider. Manual records are no longer created or used. Legacy paper records remain securely archived until their destruction date.

4.23. Off-site enrolment and data collection must be completed digitally using secure TRS systems. Staff must ensure devices are protected and data is not stored locally. Staff must take extra care when collecting data off premises for the purposes of enrolment, or other similar functions, to ensure the security of the data. Data must not be kept in vulnerable areas for any long periods, this includes cars, laptop bags or files in public areas.

4.24. Legacy paper records are securely archived and destroyed once retention periods expire.

4.25. Staff must not discuss confidential information outside work or engage in gossip that could breach confidentiality. Staff are also reminded that the nature of their work means that they will become party to information that is of a sensitive and confidential nature. In particular, employees are reminded that they should not discuss any aspect of any client's affairs or matters outside work and must not become involved in gossip involving clients whilst in work as such conversations can be overheard and could result in a serious breach of privacy and confidentiality which could affect the relationship with the client

Retention and Disposal of Data

4.26. TRS retains personal data only for as long as necessary for the purpose it was collected.

4.27. Data may be retained longer for statistical purposes where appropriate safeguards are in place.

4.28. Marketing leads and applications are retained for **6 months** unless progressed.

4.29. Personal data is disposed of securely in line with UK GDPR.

4.30. Retention periods:

- Staff records: **6 years** after leaving
- DBS certificates: destroyed within **6 months**; DBS number retained for renewal and for 6 years after leaving
- Learner records: retained for **6 years from the end of the financial year** in which final funding payment was made, or as per the funding authority contract
- Complaints: retained for as long as legally necessary

4.31. Safeguarding records: retained for **6 years** after the learner leaves TRS.

4.32. Staff receive data protection training at induction and annually thereafter.

4.33. Employers' intellectual property observed during training is kept confidential and redacted in learner work.

4.34. Breaches of this policy may result in disciplinary action and may be reported to authorities.

4.35. All staff must follow TRS's digital security and clear-desk guidance. Failure to do so may constitute gross misconduct.

4.36. TRS reports notifiable data breaches to the ICO within **72 hours**.

5. Roles and Responsibilities

5.1. TRS's ICO registration number is **ZA123990**. The Data Protection Officer (DPO) can be contacted at **info@trstraining.net**.

5.2. Managers and supervisors must promote good information-handling practices.

5.3. Senior Management is responsible for ensuring TRS complies with UK GDPR.

5.4. Senior Management oversees the SAR Procedure and provides clarification on data protection matters.

5.5. Compliance with data protection legislation is the responsibility of all learners, employers, partners, contractors and staff.

5.6. All individuals must ensure personal data they provide to TRS is accurate and up to date.

6. Policy Monitoring and reporting arrangements

6.1. Senior Management reviews the Data Inventory annually and following any DPIAs.

6.2. The Board will review any Subject Access Requests as part of Strategic Objective 1.

6.3. The Board are responsible for approving this policy

6.4. The policy is reviewed annually.

7. Summary of Revisions

Version	Date	Revision
26-1	14/08/2026	Full section-by-section update. Modernised for UK GDPR, ESFA 24/25, KCSIE 2024. Updated lawful bases, retention, SAR timelines, DPIA triggers, breach reporting, digital-only model, security controls (MFA, encryption, zero-trust). Removed paper-based processes. Added standalone Privacy Notice, SAR Procedure, Retention

		Schedule, DPIA Procedure, Breach Procedure. Added staff-friendly and learner-friendly versions.
25-1	09/01/2025	Manual records removed; safeguarding disclosure clarified; logo updated; personnel record section added; clear desk guidance removed.
23-3	20/12/2023	Structural updates; marketing opt-out added; retention updates; consent wording updated.
23-2	31/03/2023	Added marketing lead retention; opt-out options; clarified consent.
22-1	12/01/2023	Updated job titles; approved for use.

DATA PRIVACY NOTICE

1. Purpose of this Notice

This Privacy Notice explains how TRS Training Limited collects, uses, stores and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
It applies to all learners, applicants, employers, staff and stakeholders whose personal data we process.

2. How to Contact Us

Data Protection Officer (DPO)
Email: info@trstraining.net
Telephone: **01744 809010**
Address: TRS Training Ltd, Unit 4 Micklehead Business Village, St Michaels Road, Sutton Manor, St Helens, WA9 4YU

3. The Personal Data We Collect

We may collect the following categories of personal data:

- Personal details (name, address, date of birth, gender, NI number, ULN, contact details)
- Nationality and residency information
- Residency card information
- Ethnicity
- Household information
- Previous qualifications, employment and education history
- Employment details (company, job role, contracted hours, length of employment)
- Unemployment details (benefits, duration, Jobcentre information)
- Learning difficulty and/or disability information
- Health, wellbeing and medical information
- Education, Health and Care Plan (EHCP) information
- Additional support needs
- Family/emergency contact details
- Learner Records Service (LRS) data
- Personal, career and progression objectives
- Information, Advice and Guidance (IAG) outcomes
- Attendance, progression and achievement data
- Interview records
- Visual images (CCTV, photographs)
- Offences, alleged offences, criminal proceedings and outcomes
- Information from multi-agency partners (Probation, Social Services, Mental Health services, etc.)

4. Where We Obtain Your Data

- Directly from you
- Your employer
- Learner Records Service
- Multi-agency partners
- Awarding Organisations
- ESFA / Department for Education
- DWP
- Funding authorities

5. How We Use Your Data

We process personal data for:

- Learner Records Management
- Examinations and achievement

- Safeguarding
- Funding claims
- Learner support
- Learning systems (PICS, OneFile, SharePoint, other curriculum specific learning platforms)
- Quality assurance
- Marketing and publicity (with consent)

6. Lawful Bases for Processing

We process personal data under:

- **Contract** (ESFA, awarding organisations, employer agreements)
- **Legal obligation** (safeguarding, Prevent, DBS, HMRC)
- **Public task** (funded education delivery)
- **Vital interests** (emergency situations)
- **Legitimate interests** (quality assurance, employer engagement)
- **Consent** (marketing, optional photographs, optional wellbeing disclosures)

7. Sharing Your Data

We may share data with:

- Family or representatives
- Employers
- Awarding Organisations and EPAOs
- DfE / Funding authorities
- DWP
- LRS
- Healthcare, social care and welfare organisations
- Local authorities and government bodies
- Police, Probation and Counter Terrorism Police
- Survey organisations
- Careers Service
- Community organisations
- Professional advisers

All third parties must comply with UK GDPR and have appropriate security measures.

8. Retention Periods

Retention periods follow ESFA rules and TRS policy:

- Learner records: **6 years from the end of the financial year** in which final funding payment was made, or as per the funding authorities contractual requirements
- Safeguarding records: **6 years after the learner leaves**
- Staff records: **6 years after leaving**
- DBS certificates: destroyed within **6 months**
- Complaints: retained as long as legally necessary
- Marketing leads: **6 months** unless progressed

9. Your Rights

You have the right to:

- Access your data
- Rectify inaccurate data
- Request erasure (where applicable)
- Restrict processing
- Data portability
- Object to processing
- Object to automated decision-making

- Complain to the ICO

10. Complaints

If you wish to complain about how TRS processes your data, contact:
Data Protection Officer Email: **info@trstraining.net**
You may also contact the **Information Commissioner's Office (ICO)**.

DATA SUBJECT ACCESS REQUEST PROCEDURE

1. Purpose
This procedure explains how individuals can request access to personal data held by TRS Training Limited.

2. How to Submit a Request
Requests may be submitted:
By email: info@trstraining.net
By post: Data Protection Officer TRS Training Ltd Unit 4 Micklehead Business Village St Michaels Road Sutton Manor St Helens WA9 4YU

3. Information Required
- Full name
- Date of birth
- Current address
- Contact number
- Details of the data requested
- Proof of identity (government-issued ID and proof of address)

If a representative is acting on your behalf, written authorisation is required.

4. Processing Your Request

- TRS will acknowledge your request within **5 working days**.
- TRS will respond within **one month** (UK GDPR requirement).
- Complex requests may be extended by **up to two months**.
- TRS may request additional information to verify identity or locate data.
- All SARs are logged in the **SAR Register**.

5. How Data Will Be Provided
Data will be provided securely via encrypted digital transfer.

6. Refusal of Requests
Requests may be refused if:
- They are manifestly unfounded or excessive
- Identity cannot be verified
- Disclosure would breach another person's rights

A written explanation will be provided.

7. Complaints
Complaints may be made to:
Data Protection Officer info@trstraining.net
Or to the **ICO**.

DATA RETENTION SCHEDULE

1. Purpose

This schedule outlines how long TRS retains different categories of personal data.

2. Retention Periods

2.1. Learner Data

- Government-funded learner records: **6 years from the end of the financial year** in which final payment was made or as per the funding authority's contractual requirements
- Safeguarding records: **6 years after the learner leaves**
- Achievement and assessment data: **6 years**
- Attendance data: **6 years**
- Portfolios (digital): retained in line with funding and awarding organisation rules, then securely deleted

2.2. Staff Data

- Personnel files: **6 years after leaving**
- DBS certificates: destroyed within **6 months**
- DBS number: retained for renewal and for **6 years after leaving**
- Payroll and tax records: **6 years**

2.3. Employer Data

- Contracts for Services: **6 years after contract end**
- Employer engagement records: **6 years**

2.4. Marketing Data

- Leads and enquiries: **6 months** unless progressed

2.5. Complaints

- Retained for as long as legally necessary (minimum **6 years**)

2.6. Archived Legacy Paper Files

- Retained until destruction date, then securely shredded
- No new paper records are created

3. Secure Disposal

- Digital data: securely deleted from systems
- Legacy paper data: shredded as confidential waste

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

1. Purpose

To ensure TRS identifies and mitigates high-risk data processing activities.

2. When a DPIA Is Required

A DPIA is required when processing may pose high risk, including:

- New digital systems
- AI-enabled tools
- Biometric data
- Large-scale processing
- Sensitive data
- New safeguarding processes
- New marketing technologies

3. DPIA Steps

1. Describe the processing
2. Assess necessity and proportionality
3. Identify risks
4. Identify mitigation measures
5. Consult stakeholders
6. Approve through Senior Management
7. Escalate to Board if high risk remains
8. Refer to ICO if required

4. Record Keeping

All DPIAs are logged in the **DPIA Register**.

DATA BREACH RESPONSE PROCEDURE

1. Purpose

To ensure TRS responds quickly and effectively to personal data breaches.

2. What Is a Data Breach?

Any incident leading to:

- Unauthorised access
- Loss
- Destruction
- Alteration
- Disclosure of personal data.

3. Immediate Actions

1. Report the breach immediately to info@trstraining.net
2. Contain the breach
3. Secure systems
4. Preserve evidence
5. Assess risk

4. Reporting to the ICO

TRS reports notifiable breaches to the ICO within **72 hours**.

5. Communication with Data Subjects

If the breach poses high risk, affected individuals will be informed promptly.

6. Record Keeping

All breaches are logged in the **Breach Register**.

How We Use Your Information (Learner Guide)

Why we collect your information

We collect information about you so we can:

- enrol you on your course
- support your learning
- keep you safe
- claim funding from the government
- record your progress and achievements

We only collect what we need.

What information we collect

This may include:

- your name, address and contact details
- date of birth and nationality
- employment or unemployment details
- previous qualifications
- learning support needs
- health or wellbeing information (if you choose to share it)
- emergency contact details
- attendance, progress and achievement
- safeguarding information (if needed)

How we keep your information safe

TRS is a fully digital provider. Your information is stored securely in:

- PICS
- OneFile
- SharePoint
- Learning platforms
- Awarding Organisation platforms

We use strong security measures, including passwords, multi-factor authentication and encrypted systems.

Who we share your information with

We may share information with:

- your employer
- awarding organisations
- learning platform providers
- the Department for Education / DWP / Funding Authorities
- the Learner Records Service
- safeguarding partners (if needed)
- support services (if relevant)

We only share information when necessary and always securely.

Your rights

You have the right to:

- see the information we hold about you
- ask us to correct anything that is wrong
- ask us to delete information (in some cases)

- ask us to stop using your information
- ask for a copy of your information
- complain if you are unhappy with how your data is used

To use any of these rights, email: **info@trstraining.net**

How long we keep your information

- Learner records: 6 years
- Safeguarding records: 6 years after you leave
- Photos or marketing consent: only if you agree

If you have questions

Speak to your trainer or email our Data Protection Officer: **info@trstraining.net**