TSC 009 Data Protection Policy (v4.1)
Version: 4.1
Published / Effective: 26 August 2025
Policy Owner: Data Protection Officer (DPO)
Approver: Senior Information Risk Owner (SIRO – Board Lead for Data Protection)

INTRODUCTION

Purpose

The Skills Centre (TSC) is committed to being transparent about how it collects, uses and protects personal data, and to meeting its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This Policy sets out our commitments, roles and controls.

Data Protection Officer (DPO) and escalation

Public contact: dpo@theskillscentre.co.uk | 020 4613 1700.
The DPO informs and advises TSC, monitors compliance and acts as the primary contact for the Information Commissioner's Office (ICO). During DPO absence, the Deputy DPO acts under delegated authority. Unresolved risks escalate to the Senior Information Risk Owner (SIRO) (Board Lead for Data Protection).

SCOPE

This Policy applies to all personal data processed by TSC in any format and to all staff, workers, contractors and processors acting for TSC.

Plain English and abbreviations (house style)

We write in plain English. On first use, we spell out the term and put the abbreviation in brackets — for example, Data Protection Impact Assessment (DPIA) — and use the abbreviation thereafter. A short Glossary is at Appendix B.

1. DEFINITIONS (summary)

Personal data; special-category data; controller; processor; processing; UK GDPR; Data Protection Act 2018; ICO; European Economic Area (EEA). See Appendix B for plain-English explanations.

2. STAFF OBLIGATIONS

All staff must: complete training; follow this Policy and local procedures; keep personal data confidential; only use it for legitimate purposes; report incidents without delay.

2.1 Policy availability and training

This Policy is provided at induction and refreshed periodically. All staff complete data-protection training on induction and at regular intervals; updates and material changes are cascaded.

3. DATA PROTECTION PRINCIPLES

We apply: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.

4. LAWFUL USE OF PERSONAL DATA
We identify and record a lawful basis for each processing activity in our Record of Processing Activities (RoPA). For special-category data, we identify an Article 9 condition and maintain an Appropriate Policy Document (APD) where required. Changes to processing are assessed by the DPO; privacy notices and records are updated when needed.

4.1 Learner identity fields
'Sex' for the Individualised Learner Record (ILR) is recorded at enrolment only and must follow ILR codes (M/F). Pronouns are optional at enquiry and used only for communications. We do not automatically map enquiry fields (including Sex/Pronouns) into ILR fields.

5. TRANSPARENT PROCESSING – PRIVACY NOTICES UNDER THE UK GDPR
We provide clear privacy information at or before data collection. Current notices include learners, staff and applicants, employers and suppliers. Where we obtain data from other sources, we provide a notice within one month where required; if our purposes or lawful bases change, we update the notices and records.

5.1 Learner Privacy Notice (authoritative)
This Policy sets principles and governance; the Learner Privacy Notice (online) is the authoritative transparency statement for learners (purposes, lawful bases, recipients, retention and rights). If there is any divergence, the Learner Privacy Notice prevails on transparency statements; this Policy prevails on governance and controls. The current version and 'Last updated' date are shown on the webpage.

5.2 Version control and change log
We keep a Policy/Notice change log recording Published and Effective dates. Material changes to notices are highlighted and cascaded via learner-facing touchpoints.

5.3 Where to find it
The current Learner Privacy Notice is on our website and referenced in enrolment forms, learner portals and notification emails.

6. RECORDS OF PROCESSING ACTIVITIES (RoPA)
We maintain an up-to-date RoPA covering purposes, categories of data/subjects, recipients, transfers, retention, security and lawful bases. Each record has a named Owner, a review cadence and evidence of updates.

6.1 Data quality – operational
When collecting and recording personal data, staff must:

- record information accurately and keep it up to date;
- limit collection to what is adequate, relevant and necessary for the stated purpose;
- when receiving data from external sources, take reasonable steps to confirm it is accurate, up to date and not excessive for the purpose;
- review and maintain records so they remain accurate and relevant; do not alter records that must be preserved in original form (e.g., for legal reasons or investigations).

7. RETENTION AND DELETION
We retain personal data only as long as necessary for the stated purposes, following our Retention Schedule. Deletion is secure and evidenced.

7.1 ILR retention split

- **ILR (provider-held)**: retain only what is necessary to evidence delivery/funding in line with **ESFA** (Education and Skills Funding Agency) / **DfE** (Department for Education) rules.
- **ILR (DfE-held)**: the DfE retains ILR operationally for up to **20 years** and for research **to age 80**. **We do not mirror** DfE retention locally unless specifically justified and minimised.

8. DATA SECURITY
We implement proportionate technical and organisational measures across collection, storage, transmission and disposal (for example, access controls, encryption, configuration management, monitoring and testing).

8.1 Special-category safeguards
Special-category data is role-based and need-to-know, with audit logging and periodic permission reviews evidenced.

8.2 Ownership and change governance
Each key system has a named Owner, a documented review cadence for access and security settings, and a change-approval process. Change/audit logs are retained to evidence access and edits.

9. PERSONAL DATA BREACH
A personal data breach is any security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Staff must follow the Incident/Breach procedure.

9.1 We assess without undue delay and, where a notifiable breach has occurred, **notify the ICO within 72 hours of becoming aware.** If notification cannot be made within 72 hours, we document the reasons for the delay. Actions and decisions are recorded in the Incident/Breach Register.

9.2 Legal holds and evidence preservation
Where required, we apply legal holds and evidence-preservation steps and record the rationale. Examples include confidentiality (unauthorised disclosure/access), availability (loss of access/destruction) and integrity (unauthorised alteration) breaches.

10. APPOINTING PROCESSORS AND SYSTEMS
We use processors only where due diligence and Article 28 contracts are in place (confidentiality; security; sub-processor controls; assistance with rights/DPIAs/breaches; deletion/return; audit rights).

10.1 Processors & Systems Register
We maintain an authoritative register of core categories (for example, Management Information System (MIS), Microsoft 365, e-portfolio/assessment, marketing and events, analytics, hosting). Annual due-diligence/contract checks apply. Sub-processor disclosures are monitored and material changes trigger review. Configuration reviews (access, roles, security settings) run to cadence with evidence filed.

11. INDIVIDUALS' RIGHTS

11.1 SARs – time and fees
We respond within **one month** of receipt and may **extend by up to two further months** where requests are complex or numerous (we will tell you within one month if we need more time). We **do not charge a fee** unless a request is **manifestly unfounded or excessive**. Verification uses a continuity/challenge code before documentary ID, and disclosures are provided securely with the password sent separately.

11.2 Clarification pause
If we reasonably require clarification due to volume or ambiguity, the time limit pauses until clarification is received (recorded in the SAR Tracker).

11.3 Marketing objections
Marketing objections are honoured promptly and suppression lists are enforced.

12. MARKETING AND THE PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS (PECR)

Direct marketing must comply with UK GDPR and PECR. Email/SMS to individuals requires consent or soft opt-in; every message includes an opt-out. Corporate subscribers are treated under PECR rules for corporates. Newsletters and similar use consent; event invites to known contacts may rely on soft opt-in where applicable. Suppression lists are maintained and enforced.

13. AUTOMATED DECISION-MAKING, PROFILING AND AI

13.1 No solely automated decisions
No solely automated decision-making that produces legal or similarly significant effects for employees or learners.

13.2 Use of AI and large language model (LLM) tools
Any use of AI (including generative AI or automated analytics) involving personal data requires **DPO approval**, **a Data Protection Impact Assessment (DPIA) and, where applicable, a Transfer Risk Assessment (TRA). V**endor assessments are recorded in the **Processors & Systems Register** and **the Vendor & Transfers Register**. Prompt/content logs must be minimised; no training of external models on our personal data.

14. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)
DPIAs are required where processing is likely to result in high risk to individuals. They describe processing, assess necessity and proportionality, identify risks and set mitigations. The DPO reviews DPIAs; residual high risk may require prior ICO consultation. Design cycle: RoPA baseline > DPIA > Legitimate Interests Assessments (LIAs) > APD > Policy > Privacy Notice > RoPA final.

15. INTERNATIONAL TRANSFERS

15.1 Transfer mechanisms
Restricted transfers outside the UK require appropriate safeguards: Adequacy Regulations, the International Data Transfer Agreement (IDTA), or the UK Addendum to the EU Standard Contractual Clauses (SCCs). Staff must not transfer personal data internationally without DPO approval.

15.2 Approval and recording
The Vendor & Transfers Register records the hosting region(s), transfer mechanism used, relevant sub-processors, and last review date.

15.3 Transfer Risk Assessment (TRA)
For non-adequacy transfers, we complete a TRA and record hosting regions, mechanism, sub-processors and last review date in the Vendor & Transfers Register.

16. HOW OUR GOVERNANCE INTERCONNECTS (single source of truth)
Policy > APD > RoPA > DPIA Register > LIA Register > Retention Schedule > Processors & Systems Register > Vendor & Transfers Register > SAR Tracker > Incident/Breach Register > Privacy Notices.

16.1 Document authority and change log
Where this Policy and a live register differ, this Policy prevails for principles and the live register prevails for operational detail. We keep a change log that records Published and Effective dates for this Policy and for each Privacy Notice; material changes are highlighted. Document order: Policy > APD / Privacy Notices > Registers > SOPs & Templates.

Appendix A – Appropriate Policy Document (APD) (extract)
We maintain a standalone APD setting out: purposes and lawful bases for special-category data; conditions relied upon; retention; access controls; security measures; review cadence; DPO contact. The APD file is the controlled master.

Appendix B – **Glossary of Terms (Plain English)**
APD – Appropriate Policy Document: explains why we can process special-category data and how we protect it.
DPO – Data Protection Officer: TSC's independent data-protection adviser and ICO contact.
Deputy DPO: covers when the DPO is unavailable.
SIRO – Senior Information Risk Owner: Board lead for information risk and data protection.
RoPA – Record of Processing Activities: our master list of what personal data we process, why and how it's protected.

DPIA – Data Protection Impact Assessment: a risk assessment we do before starting high-risk processing.
LIA – Legitimate Interests Assessment: shows how we balance our interests with the individual's rights.
ILR – Individualised Learner Record: the DfE dataset used to fund and track further-education learners.
DfE – Department for Education (UK).
ESFA – Education and Skills Funding Agency: an agency of DfE.
ICO – Information Commissioner's Office: the UK data-protection regulator.
UK GDPR – UK General Data Protection Regulation.
PECR – Privacy and Electronic Communications Regulations: rules on electronic marketing and cookies.
TRA – Transfer Risk Assessment: check we do for international data transfers to non-adequate countries.
IDTA – International Data Transfer Agreement (UK).
SCCs – Standard Contractual Clauses (EU) with UK Addendum.
MIS – Management Information System: our learner/centre database [PICS].
SAR – Subject Access Request: a request to see personal data we hold.
FYE – Financial Year End.
LLM – Large Language Model: a type of AI system for text generation/analysis.

Change log (extract)
4.1 (26 Aug 2025): Added policy/notice authority and change log; Deputy DPO cover and SIRO escalation; learner identity fields (ILR Sex/pronouns); special-category safeguards; ILR provider vs DfE retention split; TRA requirement; Processors & Systems Register expectations; SAR clarification pause; breach legal holds; security ownership/change governance; AI/LLM safeguards; plain-English abbreviation rule; Glossary added.