

TSC 009 Data Protection Policy

Version: 4.2

Published / Effective: 1 September 2026

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), the Data Protection Act 2018 (DPA 2018), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), and the amendments made by the Data (Use and Access) Act 2025 (DUAA). 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). The DPO performs these duties independently, reports to the highest management level and is involved promptly in matters affecting personal data. During DPO absence or vacancy, documented cover is provided by an appointed deputy or external DPO service. 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; criminal-offence data; controller; processor; joint controller; processing; UK GDPR; DPA 2018; DUAA; PECR; ICO; European Economic Area (EEA); recognised legitimate interests; and automated decision-making (ADM). 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; use only approved systems and AI tools for personal data; recognise and promptly route rights requests and data protection complaints; 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. Training covers rights requests, data protection complaints, incidents, secure handling, direct marketing and approved AI use where relevant to the role.

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). Where we rely on recognised legitimate interests, we record the relevant statutory condition and why the processing is necessary. A balancing test is not required, but all other UK GDPR duties, including the right to object, continue to apply. For special-category data, we identify an Article 9 condition and maintain an Appropriate Policy Document (APD) where required. For criminal-offence data, we identify the relevant Article 10 and DPA 2018 Schedule 1 condition and maintain an APD where required. Changes to processing, including reuse for a new purpose, are assessed by the DPO for lawfulness and compatibility; 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. Where relevant, notices identify recognised legitimate interests, significant automated decision-making, international transfers and the route for making a data protection complaint.

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, Article 6 lawful bases, any recognised legitimate-interest condition, and any applicable Article 9 or Article 10/DPA 2018 Schedule 1 condition. 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. Legal holds, investigations and contractual or regulatory requirements suspend scheduled deletion where necessary, with the reason and review date recorded.

7.1 ILR retention split

- ILR (provider-held): retain only what is necessary to evidence delivery/funding in line with applicable Department for Education (DfE), devolved or combined-authority, awarding-organisation and contractual rules.
- ILR (DfE-held): the current DfE ILR Privacy Notice states that DfE retains ILR learner data for 20 years for operational purposes and in research databases until the learner is aged 80. TSC does not mirror that period locally unless the retention is justified, documented 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 and criminal-offence safeguards

Special-category and criminal-offence data are 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.

8.3 Data protection by design and default

New systems, forms, sharing arrangements and material changes must minimise personal data and build in access, retention, security and rights controls from the outset. Where an online

service is likely to be accessed by children, its design must take their needs into account and support their protection.

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 breaches without undue delay. Where a breach is likely to result in a risk to individuals' rights and freedoms, we notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. If notification is later, we document the reasons. Where a breach is likely to result in a high risk, we notify affected individuals without undue delay unless a legal exception applies. 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). Processor arrangements also require prompt escalation and support for rights requests and data protection complaints received by or involving the processor.

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.

10.2 Data sharing and controller relationships

Before personal data is shared with an independent or joint controller, TSC records the parties' roles, purpose, lawful basis, data categories, security, retention, rights handling and international-transfer position. Joint-controller responsibilities are allocated in a written arrangement. A Data Sharing Agreement (DSA) is used for regular, high-risk or complex sharing where appropriate.

11. INDIVIDUALS' RIGHTS

TSC facilitates the rights of access, rectification, erasure, restriction, portability and objection, and rights relating to automated decision-making, subject to legal conditions and exemptions. Requests may be verbal or written and do not require legal wording. Staff must send any rights request to the DPO without delay.

11.1 SARs – time and fees

We respond without undue delay and within one month of receipt, or within one month after receiving any reasonably requested identity or authority information, or a required fee. We may extend by up to two further months where necessary because a request is complex or the person has made several requests; we tell the person within the initial period and explain why. We make reasonable and proportionate searches. We normally charge no fee, but we may charge a reasonable administrative fee or refuse to act where a request is manifestly unfounded or excessive; a reasonable fee may also be charged for further copies. Any refusal is documented and explained, including complaint and court rights. Identity verification is reasonable and proportionate. We use existing account or challenge information before documentary ID where practicable. Disclosures are provided securely, with passwords or equivalent credentials sent separately where used.

11.2 Clarification pause

If clarification is reasonably required because TSC holds a large amount of information or the request is unclear, the time limit pauses on the day we ask and resumes the day after we receive the clarification. We do not require a person to narrow a valid request. The pause and reason are recorded in the SAR Tracker.

11.3 Marketing objections

Marketing objections are honoured promptly and suppression lists are enforced.

11.4 Data protection complaints

TSC provides clear electronic and non-electronic routes for data protection complaints, including dpo@theskillscentre.co.uk. We acknowledge receipt within 30 days. Without undue delay, we make appropriate enquiries, keep the complainant informed, and explain the outcome and any action taken. Complaints are recorded in the Data Protection Complaints Register, and the final response explains the right to complain to the ICO.

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

Direct marketing must comply with UK GDPR and PECR. Unsolicited email, SMS and other electronic-mail marketing to individual subscribers, including sole traders and some partnerships, requires consent unless all conditions of the products-and-services soft opt-in are met. Those conditions include obtaining the details directly during a sale or negotiation for a sale, marketing TSC's similar services, and giving a clear opt-out when the details are collected and in every message. Corporate subscribers do not require consent under the PECR electronic-mail rule, but TSC identifies itself, provides a valid unsubscribe route, respects objections where personal data is used, and enforces suppression lists. Newsletters and event invitations follow the same rules according to the recipient type and how the details were obtained. Live marketing calls are screened against the Telephone Preference Service and Corporate Telephone Preference Service and against prior objections; automated marketing calls require consent.

12.1 Storage and access technologies

Cookies and similar technologies require consent unless a PECR exception applies. When TSC relies on the statistical-purpose or appearance/functionality exceptions, it provides clear information and an easy way to object. Uses are recorded and reviewed through the website and cookie-governance process.

13. AUTOMATED DECISION-MAKING, PROFILING AND AI

13.1 No solely automated decisions

TSC does not permit solely automated decision-making that produces legal or similarly significant effects for employees, applicants or learners unless the SIRO and DPO approve a documented exception. Any exception must have a lawful basis, a DPIA, clear privacy information, and safeguards allowing the person to make representations, challenge the decision and obtain meaningful human intervention. The use of special-category data is subject to the stricter statutory conditions.

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). Vendor 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. Personal data must not be entered into unapproved AI services. Human review is required where AI output informs a decision affecting an individual. Contracts, service settings and technical controls must prevent provider training on TSC personal data unless separately assessed and approved.

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. If high risk remains after mitigation, TSC must consult the ICO before processing unless the processing is not pursued. Typical design cycle: RoPA baseline > screening and DPIA where required > lawful-basis assessment, including an LIA or recognised legitimate-interest necessity assessment where relevant > APD where required > controls and privacy information > final RoPA update.

15. INTERNATIONAL TRANSFERS

15.1 Transfer mechanisms

Restricted transfers outside the UK require one of the following routes: UK adequacy regulations; appropriate safeguards such as the International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses (SCCs), or binding corporate rules, together with a completed data protection test/TRA; or a documented Article 49 exception. Staff must not initiate a restricted transfer without DPO approval.

15.2 Approval and recording

The Vendor & Transfers Register records the hosting region(s), transfer mechanism used, relevant sub-processors, onward-transfer position, data protection test/TRA outcome, supplementary measures, and last review date.

15.3 Transfer Risk Assessment (TRA)

For restricted transfers relying on appropriate safeguards, we complete a TRA to decide, acting reasonably and proportionately, that the standard of protection after transfer is not materially lower than in the UK. Any supplementary contractual, technical or organisational measures are implemented and recorded before the transfer.

16. HOW OUR GOVERNANCE INTERCONNECTS (single source of truth)

Policy > APD > RoPA > DPIA Register > LIA Register > Retention Schedule > Processors & Systems Register > Vendor & Transfers Register > DSA Register > SAR Tracker > Data Protection Complaints Register > 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 and criminal-offence data where required; Article 9 and DPA 2018 Schedule 1 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 process special-category and, where required, criminal-offence data and how we protect it.

DPO – Data Protection Officer: TSC's independent data-protection adviser and ICO contact.

DPO cover: the appointed deputy or external service providing documented cover when the DPO is unavailable or the post is vacant.

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.

Recognised legitimate interest: an Article 6 lawful basis for specified public-interest purposes, including safeguarding, crime prevention and emergencies. It requires a necessity assessment but not a balancing test.

ILR – Individualised Learner Record: the DfE dataset used to fund and track further-education learners.

DfE – Department for Education (UK).

ESFA – former Education and Skills Funding Agency: closed on 31 March 2025, with its functions moved into DfE.

ICO – Information Commissioner's Office: the UK data-protection regulator.

UK GDPR – UK General Data Protection Regulation.

DPA 2018 – Data Protection Act 2018.

DUAA – Data (Use and Access) Act 2025: legislation that amended the UK GDPR, DPA 2018 and PECR.

PECR – Privacy and Electronic Communications Regulations: rules on electronic marketing and cookies.

TRA – Transfer Risk Assessment: the assessment used to meet the international-transfer data protection test when TSC relies on appropriate safeguards.

Data protection test: the requirement to decide, reasonably and proportionately, that protection after a restricted transfer is not materially lower than in the UK.

IDTA – International Data Transfer Agreement (UK).

SCCs – Standard Contractual Clauses (EU) with UK Addendum.

MIS – Management Information System: our learner/centre database ~~[PICS]~~ (for example, PICS).

SAR – Subject Access Request: a request to see personal data we hold.

ADM – Automated decision-making: a decision made using automated processing, including profiling, with no meaningful human involvement in the decision itself.

Data protection complaint: a concern that TSC has infringed data protection law in the way it handled a person's personal data.

DSA – Data Sharing Agreement: a written record of the purpose, roles and controls for a data-sharing arrangement.

FYE – Financial Year End.

LLM – Large Language Model: a type of AI system for text generation/analysis.

Change log (extract)

4.2 (draft reviewed 1 Sep 2026): aligned the Policy with DUAA changes in force; added the statutory data protection complaints process, reasonable and proportionate SAR searches, recognised legitimate interests, automated-decision safeguards, children's online-service design requirements and PECR storage/access exceptions; updated international transfers, data-sharing controls, breach communication, DfE/ESFA references, individual rights, criminal-offence data and version control.

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.