Data Protection and GDPR Policy 2026-2027

Document Control

Field	Details
Author	Head of Operations and Compliance
Document owner	Head of Operations and Compliance
Executive owner	Chief Executive Officer
Approved by	Senior Management Team
Partner institution	University of West London (UWL), where applicable
Reference	P013-30092026-v6.0
Version	6.0
Effective date	01 September 2026
Review date	31 July 2027
Classification	Public, with internal procedures and registers classified separately
Regulatory Framework	UK GDPR; Data Protection Act 2018; Data (Use and Access) Act 2025; PECR; Apprenticeship Funding Rules 2026 to 2027; ILR requirements; safeguarding information-sharing guidance

1. Policy Statement

Supply Chain Academy Limited (SCA) is committed to protecting personal data and respecting the privacy rights of apprentice learners, prospective learners, employees, workers, employers, clients, suppliers, partners and other individuals whose information it processes.

SCA will process personal data lawfully, fairly, transparently and securely. Data protection will be embedded in governance, apprenticeship delivery, safeguarding, learner support, employer engagement, quality assurance, information technology, procurement and partnership working.

This policy establishes SCA's organisation-wide framework. Processing-specific information is provided through privacy notices, contracts, consent statements where appropriate, and internal procedures and registers.

2. Purpose

The purpose of this policy is to:

- define SCA's commitment to compliance with data protection law;
- set out the principles, responsibilities and controls that apply to personal data;
- explain how SCA manages apprentice, learner, employee and business information;
- ensure privacy risks are identified and addressed before new processing begins;
- provide a framework for information rights, complaints, breaches, retention, sharing and international transfers; and
- support accountability to individuals, regulators, funders, partners and the Senior Management Team.

3. Scope

This policy applies to all SCA employees, workers, directors, temporary staff, contractors, consultants, volunteers, apprentices acting on SCA's behalf, and third parties who process personal data for SCA. It applies to personal data in any format, including digital records, email, paper files, photographs, audio, video, learning-platform data, recordings, system logs and information generated or analysed using artificial intelligence.
The policy covers SCA-controlled systems and approved processing undertaken through employer systems, partner systems, cloud services, remote-working arrangements and personal devices where their use has been authorised.

4. Legal and Regulatory Framework

SCA will have regard to, as applicable:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018;
- the Data (Use and Access) Act 2025;
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR);

- the Computer Misuse Act 1990 and relevant confidentiality, communications and cyber-security law;
- the Apprenticeship Funding Rules 2026 to 2027 and associated evidence requirements;
- the Individualised Learner Record specification and provider-support requirements;
- safeguarding, Prevent and information-sharing guidance; and
- contractual and data-sharing requirements involving DWP, employers, UWL, awarding bodies, end-point assessment organisations, technology suppliers and other delivery partners.

Where legal requirements, funding rules or contractual terms change during the policy year, SCA will update its procedures, privacy information and controls without waiting for the annual policy review.

5. Definitions

Personal data: information relating to an identified or identifiable living individual.

Processing: any operation performed on personal data, including collection, recording, organisation, storage, use, alteration, retrieval, consultation, disclosure, sharing, restriction, erasure or destruction.

Special category data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for unique identification, health data, sex life or sexual orientation.

Criminal offence data: personal data relating to criminal convictions, offences, allegations, proceedings or related security measures.

Controller: the organisation that determines the purposes and means of processing.

Processor: an organisation that processes personal data on behalf of a controller.

Data subject: the individual to whom personal data relates.

Personal data breach: a security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data Protection Impact Assessment (DPIA): a documented assessment used to identify and reduce risks arising from processing likely to result in a high risk to individuals.

6. Data Protection Principles

SCA will comply with the seven UK GDPR principles. Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;

- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary;
- processed securely using appropriate technical and organisational measures; and
- managed in a way that enables SCA to demonstrate accountability.

7. Accountability and Governance

SCA will demonstrate compliance by maintaining proportionate and current:

- records of processing activities and information-asset registers;
- privacy notices for learners, staff and other relevant groups;
- lawful-basis, special-category and criminal-offence condition records;
- data-retention schedules;
- data-sharing agreements and processor contracts;
- DPIAs and legitimate interests assessments where required;
- personal data breach and near-miss records;
- information-rights and data-protection complaints logs;
- training, audit and assurance records; and
- documented decisions, actions and improvement plans.

The Head of Operations and Compliance will coordinate SCA-level compliance and liaison with the Group Data Protection Officer. Formal statutory DPO responsibilities will remain with the person or function designated by the Group where the legal criteria for appointment apply.

8. Roles and Responsibilities

8.1 Senior Management Team

- approve this policy and ensure adequate resources;
- receive assurance on significant privacy risks, breaches, complaints and improvement actions;
- ensure data protection is integrated into governance, risk management and quality assurance; and
- support a culture in which concerns may be raised promptly and without detriment.

8.2 Head of Operations and Compliance

- maintain SCA's policy framework, processing register and retention arrangements;
- coordinate rights requests, complaints, DPIAs, breaches and audits with the Group DPO;
- ensure learner, employer and partner processing is documented;
- monitor completion and impact of staff training; and
- report material risks and non-compliance to senior leaders.

8.3 IT and System Owners

- implement appropriate access, security, resilience, backup and recovery controls;

- maintain system and supplier assurance;
- remove or amend access promptly when roles change;
- support breach investigation, evidence preservation and secure deletion; and
- ensure new systems and material changes follow privacy-by-design and change-control requirements.

8.4 All Staff and Contractors

- access personal data only where authorised and necessary;
- use approved systems, accounts and communication methods;
- follow confidentiality, clear-desk, secure-transfer and disposal requirements;
- check recipient details and attachments before sending information;
- report actual or suspected breaches immediately;
- complete required training and cooperate with audits; and
- seek advice before starting unfamiliar, high-risk or materially changed processing.

9. Personal Data Processed by SCA

Depending on the relationship and purpose, SCA may process identification and contact details; employment and employer details; eligibility and residency evidence; education, skills and assessment information; attendance and engagement; progress reviews; off-the-job training evidence; learning support and reasonable-adjustment information; financial and funding data; ILR information; communications; complaints and appeals; safeguarding and Prevent information; equality and diversity monitoring data; system-security data; and destination and progression information.

SCA will collect only the information reasonably required for identified purposes and will explain the processing through the relevant privacy notice.

10. Apprentice and Learner Data

SCA processes apprentice and learner data to assess eligibility and prior learning, enrol learners, deliver and evaluate training, provide support, communicate with employers, record progress, meet funding and audit requirements, submit required returns, support assessment and end-point assessment, safeguard learners and monitor destinations and outcomes.

Information may be shared, where necessary and lawful, with the learner's employer, DWP and its delivery bodies, UWL where applicable, awarding organisations, end-point assessment organisations, subcontractors, professional bodies, auditors, regulators, safeguarding agencies and approved technology providers.

Learners under 18 will receive age-appropriate privacy information. Decisions about sharing safeguarding information will prioritise safety and best interests and will not rely on consent where another lawful basis permits or requires necessary and proportionate sharing.

11. Lawful Bases and Conditions

Before processing starts, SCA will identify and document an appropriate Article 6 lawful basis. Depending on the circumstances, this may include legal obligation, contract,

legitimate interests, public task where applicable, vital interests or consent.
Where special category data is processed, SCA will also identify an Article 9 condition and any required Data Protection Act 2018 Schedule 1 condition. Where criminal offence data is processed, SCA will identify the relevant UK GDPR and statutory authority and apply appropriate safeguards.

Consent will be used only where it is freely given, specific, informed and unambiguous, and where withdrawal can be honoured. SCA will not default to consent where processing is required by law, contract, safeguarding duties or funding requirements. Where required by law, SCA will maintain an Appropriate Policy Document for relevant Schedule 1 processing.

12. Privacy Information and Transparency

SCA will provide concise, accessible and clear privacy information at or before collection, unless a lawful exception applies. Privacy notices will explain who controls the data, purposes, lawful bases, categories, recipients, retention, international transfers, rights, complaint routes and relevant automated decision-making.

Privacy information will be reviewed when processing changes. Material changes will be communicated through an appropriate channel.

13. Individual Rights

Subject to legal conditions and exemptions, individuals have rights to be informed, access their personal data, rectify inaccurate data, erase data, restrict processing, receive portable data, object, and receive safeguards in relation to significant automated decisions and profiling.

Requests may be made verbally or in writing and do not need to use legal terminology. SCA will verify identity proportionately, clarify the request where necessary, carry out a reasonable and proportionate search, protect the rights of others and respond without undue delay and normally within one calendar month. Where legislation permits an extension, refusal or fee, SCA will explain the decision and the individual's complaint rights.

All requests must be forwarded immediately to the Head of Operations and Compliance or Group DPO and recorded in the rights-request log.

14. Data Protection Complaints

SCA will provide an accessible route for individuals to complain about the handling of their personal data. A complaint may be made verbally or in writing and will be recognised from its substance rather than its label.

SCA will:

- acknowledge receipt within 30 days;
- take appropriate steps to investigate without undue delay;

- make proportionate enquiries and consider relevant evidence fairly;
- keep the complainant informed where the investigation remains open;
- communicate the outcome without undue delay, including any remedial action;
- explain the right to complain to the Information Commissioner's Office; and
- retain an evidence-based record of the complaint, decisions, communications and outcome.

Where practicable, a person not directly involved in the matter will review or oversee the complaint. Data-protection complaints may also engage the general Complaints Policy, but will remain separately identifiable for monitoring and assurance.

15. Data Protection by Design and DPIAs

SCA will integrate data protection into the design of systems, services, projects, forms, contracts, curriculum tools and working practices. Default settings will limit access, collection, visibility and retention to what is necessary.

A DPIA screening must be completed before high-risk processing begins, including significant use of AI or profiling, systematic monitoring, biometric identification, large-scale special-category processing, new safeguarding data-sharing initiatives, substantial data matching, or a major new learner-management or digital-learning platform. Where a DPIA is required, processing must not begin until risks, controls, consultation and approval are documented.

16. Artificial Intelligence and Automated Processing

Personal, special-category, criminal-offence, safeguarding or confidential information must not be entered into an unapproved public generative-AI service. Approved AI use must have a documented purpose, lawful basis, supplier assessment, transparency arrangements, security controls and human oversight appropriate to the risk.

SCA will assess accuracy, fairness, bias, explainability, data minimisation, retention, reuse of prompts and outputs, international transfers and individuals' rights. Decisions producing legal or similarly significant effects will not be made solely by automated means unless permitted by law and supported by appropriate safeguards, including meaningful human intervention and a route to challenge the decision.

17. Data Security

SCA will apply technical and organisational measures appropriate to the nature, scope, context and risk of processing. Controls will include, where appropriate:

- role-based access and least privilege;
- strong authentication and multi-factor authentication;
- encryption in transit and at rest;
- approved, managed and securely configured devices;
- security updates, malware protection and vulnerability management;
- secure backups, restoration testing and business continuity;

- logging, monitoring and access review;
- secure sharing and transfer methods;
- prompt amendment or removal of access;
- supplier and cloud-service assurance;
- physical security and secure disposal; and
- staff awareness, phishing resilience and incident reporting.

Removable media and local device storage may be used only where authorised, necessary and appropriately protected. Personal data must not be stored in unapproved personal accounts, messaging services or devices.

18. Remote Working and Communication

Staff working remotely must protect screens, conversations, papers and devices from unauthorised access; use approved accounts and secure connections; store information only in approved locations; and follow SCA's home-working, acceptable-use and information-security requirements. Personal email and consumer messaging services must not be used for SCA personal data unless expressly approved for a documented exceptional purpose.

19. Data Sharing and Third Parties

Before sharing personal data, SCA will confirm the purpose, necessity, lawful basis, minimum information required, recipient identity, security, retention and any restrictions on further use. Routine or high-risk sharing will be documented through an appropriate agreement or protocol.

SCA will determine whether each party acts as controller, joint controller, processor or independent controller. Processor appointments must include legally compliant written terms covering instructions, confidentiality, security, sub-processors, assistance, breach notification, rights requests, deletion or return, and audit information.

Data may be shared without consent where necessary and lawful, including for safeguarding, prevention or detection of crime, legal claims, regulatory requirements or protection of vital interests. The reasons and information shared will be documented.

20. International Transfers

Personal data must not be transferred, remotely accessed or otherwise made available to a separate organisation outside the UK unless the transfer is lawful and approved through SCA's governance process.

A restricted transfer must be covered by UK adequacy regulations, appropriate safeguards such as the UK International Data Transfer Agreement, UK Addendum or binding corporate rules, or a valid statutory exception. Where appropriate safeguards are used, SCA will complete and document the required transfer assessment or data-protection test and any supplementary measures.

21. Records Retention and Disposal

Personal data will be retained only for as long as necessary for the purpose, legal and regulatory duties, apprenticeship funding and audit requirements, safeguarding needs, contractual obligations and limitation periods. SCA will maintain an approved retention schedule rather than applying a single retention period to all information.

The schedule will cover applicant, learner, ILR, funding, learning-support, assessment, employer, safeguarding, Prevent, complaints, staff, finance, contract, CCTV, breach and information-rights records. Legal holds, investigations or safeguarding needs may require retention beyond the usual period. When retention ends, data will be securely deleted, destroyed or irreversibly anonymised.

22. Personal Data Breaches

All actual or suspected personal data breaches, security incidents and near misses must be reported immediately through the approved internal route. Staff must preserve evidence, avoid unnecessary disclosure and must not investigate beyond their authority.

The authorised lead will contain and investigate the incident, establish when SCA became aware, assess risk to individuals, document decisions and coordinate remedial action.

Where a breach is likely to result in a risk to individuals' rights and freedoms, SCA will notify the ICO without undue delay and, where feasible, within 72 hours of awareness.

Where a breach is likely to result in a high risk, affected individuals will be informed without undue delay unless a lawful exception applies.

All personal data breaches will be recorded, including those not reported to the ICO, together with reasons for the notification decision, actions taken and lessons learned.

Processors must notify SCA without undue delay in accordance with their contract.

23. Monitoring, CCTV and System Logs

Monitoring must have a clear purpose and lawful basis and must be necessary, proportionate and transparent. SCA will consider less intrusive alternatives, limit access, define retention and complete a DPIA where monitoring is likely to create high risk.

Covert monitoring will be exceptional, time-limited, authorised at an appropriate senior level and undertaken only where lawful and where the purpose cannot reasonably be achieved by less intrusive means. Monitoring information will not be reused incompatibly.

24. Direct Marketing and Electronic Communications

Direct marketing will comply with UK GDPR, the Data Protection Act 2018 and PECR. SCA will document the lawful basis, obtain consent where required, verify any reliance on the soft opt-in, identify the sender, provide a simple opt-out and action objections promptly. Suppression records may be retained to ensure that individuals who object are not contacted again for marketing.

25. Training and Awareness

All staff will complete data-protection and information-security training at induction and receive refresher training at least annually. Additional role-specific training will be provided for staff handling learner records, safeguarding information, HR data, rights requests, complaints, breaches, marketing, procurement, systems or AI-enabled processing.

Training effectiveness will be evaluated through knowledge checks, scenarios, audits, incident trends, staff confidence and observation of practice.

26. Audit, Monitoring and Assurance

SCA will monitor compliance through periodic processing-register reviews, privacy-notice reviews, access checks, retention reviews, supplier assurance, DPIA follow-up, breach and complaint analysis, training records and internal audit. Significant risks, themes and overdue actions will be reported to the Senior Management Team.

Low incident numbers will not automatically be treated as evidence of effective compliance. SCA will use assurance activity, staff and learner feedback, near misses and testing to identify under-reporting or control weaknesses.

27. Non-compliance

Breaches of this policy may be addressed through disciplinary, learner conduct, contractual, capability or supplier-management procedures, as appropriate. Certain deliberate or reckless acts involving personal data may constitute criminal offences. SCA may refer suspected criminal conduct to the police, ICO or another appropriate authority.

Decisions will be based on the circumstances, evidence and applicable law.

28. Related Policies and Records

- Learner Privacy Notice and Staff Privacy Notice;
- Records Retention Schedule;
- Information Asset and Processing Register;
- Data Protection Impact Assessment procedure;
- Information Rights Request procedure;
- Data Protection Complaints procedure;
- Personal Data Breach procedure and register;
- Data Sharing and Processor Due Diligence arrangements;
- Safeguarding Policy and Prevent Policy;
- Online Safety Policy;
- Acceptable Use and IT Security arrangements;
- Complaints Policy;
- Staff Code of Conduct and learner Code of Conduct;
- Whistleblowing Policy; and
- UWL and other partnership protocols, where applicable.

29. Policy Review

This policy will be reviewed at least annually and sooner following a significant legal or regulatory change, serious breach or complaint, material change to processing, introduction of a major system or AI capability, audit finding, partnership change or identified control weakness.

The document owner will ensure that approved changes are communicated, related documents are aligned and superseded copies are controlled.

30. Contact and Reporting Routes

Questions, rights requests, data-protection complaints and suspected breaches should be reported promptly to the Head of Operations and Compliance or through the Group Data Protection Officer route published in the relevant privacy notice. Immediate security incidents must also be reported through the approved IT incident route.

Individuals may complain to the Information Commissioner's Office. SCA will not disadvantage any person for raising a genuine concern or exercising a data-protection right.

SMT APPROVAL

Date	Updates/Amendments	Signature
11/09/2023	Annual review for amendment as relevant.	**Neil Roll**
26/09/2024	Change of business name from CP Training Services Ltd to Supply Chain Academy Limited.	**Neil Roll**
16/07/2026	Policy name change and update in line with requirements and expectations of KCSIE 2026	**Makayla Whyte**
30/09/2026	Full legal and operational rewrite, including DUAA 2025, apprentice data, information rights, complaints, AI, DPIAs, international transfers, breaches and accountability.	*Makayla Whyte*