

DATA PROTECTION POLICY

Unique School Solutions Ltd

Document control	Details
Policy owner	Directors / Data Protection Lead
Data Protection Lead	Rebecca Dodd
ICO registration	ZA304371
Approved	September 2026
Next review	September 2027, or sooner if law, guidance or processing changes
Classification	Internal policy; may be shared with clients, auditors and workers

Policy statement

Unique School Solutions Ltd (USS) is committed to handling personal data lawfully, fairly, transparently and securely. We use only the personal data needed to provide education recruitment services, safeguard children and adults at risk, employ and pay staff and workers, meet legal and contractual duties, and operate our business responsibly.

This policy is designed for a UK education recruitment business and supports the accountability expectations of the Recruitment and Employment Confederation (REC) Audited Education scheme. It must be read with the USS Privacy Notice, Recruitment and Selection Policy, Safeguarding and Child Protection Policy, DBS procedures, breach-response procedure and retention schedule.

1. Purpose and scope

This policy explains the standards and controls USS applies when it processes personal data. It applies to directors, employees, temporary workers, agency workers, consultants, contractors and any person processing information on behalf of USS. It covers electronic, paper, audio, image and archived records relating to candidates, workers, employees, client contacts, referees, suppliers, website users and other stakeholders.

USS normally acts as a data controller for its recruitment, employment, safeguarding, payroll, marketing and business activities. It may act as a processor only where a written arrangement clearly requires USS to process personal data solely on another controller's instructions.

2. Legal and regulatory framework

USS will comply with applicable data protection and privacy law, including:

Unique School Solutions Ltd
Unit 3, Enterprise Court, Farfield Park, Rotherham, S63 5DB
Telephone: 0114 3392026
Company Registration Number: 10943136

- the UK General Data Protection Regulation (UK GDPR), as amended;
- the Data Protection Act 2018 (DPA 2018);
- the Data (Use and Access) Act 2025 (DUAA 2025), which amends rather than replaces the UK GDPR and DPA 2018;
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), where electronic marketing or cookies are used;
- the Employment Agencies Act 1973 and Conduct of Employment Agencies and Employment Businesses Regulations 2003;
- Keeping Children Safe in Education (KCSIE) 2026 and relevant statutory safeguarding guidance;
- the DBS Code of Practice and applicable rehabilitation-of-offenders legislation; and contractual and audit requirements applying to education recruitment

Where legal requirements conflict or an exemption may apply, USS will obtain appropriate advice and document the decision.

3. Key definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person.
Special category data	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, or data about a person's sex life or sexual orientation.
Criminal offence data	Data about criminal convictions, offences, alleged offences, proceedings or related security measures. This includes a statement that a person has no convictions.
Processing	Any operation involving personal data, including collecting, recording, organising, storing, viewing, using, sharing, changing, restricting, deleting or destroying it.
Controller	The person or organisation that determines why and how personal data is processed.
Processor	A person or organisation processing personal data on a controller's documented instructions.
Personal data breach	A security breach leading to accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to, personal data.
Data subject	The living person to whom personal data relates.

4. Governance and responsibilities

4.1 Directors and Data Protection Lead

The directors are accountable for compliance. Rebecca Dodd is the Data Protection Lead and the principal contact for rights requests, complaints and breaches info@uniqueschoolsolutions.co.uk.

USS does not describe this role as a statutory Data Protection Officer unless the legal appointment criteria are met and a formal appointment is made.

The Data Protection Lead will maintain appropriate policies records of processing, lawful-basis assessments, retention controls, processor contracts, breach records, complaint records and data protection impact assessments (DPIAs), and will arrange proportionate staff training.

4.2 All personnel

- access personal data only where needed for their role and use it only for authorised purposes;
- follow access, password, transfer, clear-desk, disposal and confidentiality controls;
- check accuracy before using or sharing information;
- refer rights requests, complaints, unusual disclosures and new high-risk processing promptly to the Data Protection Lead;
- report an actual or suspected breach immediately and preserve relevant evidence; and
- complete required training and cooperate with audits.

5. Data protection principles

USS applies the following principles to all personal-data processing:

Principle	USS standard
Lawfulness, fairness and transparency	Use data only on a valid basis, in ways people would reasonably expect, and explain processing clearly.
Purpose limitation	Collect data for specified, explicit and legitimate purposes and do not reuse it incompatibly.
Data minimisation	Use only data that is adequate, relevant and necessary.
Accuracy	Take reasonable steps to keep data accurate and current and correct or delete inaccurate data without undue delay.
Storage limitation	Keep identifiable data only for as long as it is needed and then securely delete, destroy or anonymise it.
Integrity and confidentiality	Protect data using appropriate technical and organisational measures.

Accountability	Be able to demonstrate compliance through records, controls, decisions and review.
----------------	--

6. What USS processes and why

Depending on the relationship and role, USS may process contact and identity details;

- CVs, application forms and work history;
- qualifications and professional registrations;
- references; interview and suitability records; r
- Right-to-work evidence;
- availability and assignment records;
- payroll, tax, pension and bank details;
- health, disability and adjustment information;
- equality information; safeguarding information;
- DBS and criminal-record information;
- complaints, conduct and incident records;
- public online information relevant to safeguarding;
- system and communication records; and client or supplier contact details.

USS must give individuals an appropriate privacy notice when data is obtained directly and, where data is obtained elsewhere, within the period required by law. Privacy notices will explain the purposes, data categories, lawful bases, recipients, retention approach, rights and contact details. This policy does not replace those notices.

7. Lawful bases

Before processing begins, USS will identify and record an Article 6 lawful basis. Consent will not be used merely because it appears convenient; in recruitment and employment it may not be freely given. Withdrawal of consent does not affect processing based on another lawful basis or processing already carried out lawfully.

Lawful basis	Typical USS use
Contract / pre-contract steps	Registering a candidate, introducing or supplying a worker, administering an assignment, engaging staff and delivering agreed services.
Legal obligation	Right-to-work, tax, payroll, pensions, employment, equality, agency regulation, safeguarding and required record-keeping.
Legitimate interests	Operating and improving recruitment services, maintaining business relationships, preventing misuse, defending claims and proportionate candidate sourcing or vetting, after assessing necessity and impact.

Recognised legitimate interests	Only where a processing purpose falls within the statutory recognised categories introduced by DUAA 2025 and necessity is documented.
Vital interests	Urgent processing needed to protect someone's life where another basis is unsuitable.
Public task	Only where USS is lawfully carrying out, or supporting as controller, a task in the public interest with a clear basis in law.
Consent	Genuinely optional processing, such as selected marketing activities, where consent is specific, informed and capable of withdrawal.

8. Special category and criminal offence data

An Article 6 lawful basis is not enough for special category or criminal offence data. USS must also identify an Article 9 condition and/or legal authority under Article 10 and Schedule 1 DPA 2018. Relevant conditions may include employment and social-protection obligations, substantial public interest in safeguarding children or people at risk, equality monitoring, preventing or detecting unlawful acts, legal claims, occupational health, vital interests or explicit consent where genuinely appropriate.

Where Schedule 1 requires an Appropriate Policy Document, section 22 of this policy is intended to form that document. USS will complete a DPIA where processing is likely to result in high risk, including most systematic criminal-record vetting and any new intrusive screening technology.

9. Recruitment, vetting and safeguarding

9.1 Proportionate checks

USS carries out checks needed to assess suitability for work in education and meet safeguarding, legal and client requirements. Checks must be role-relevant, proportionate, transparent and conducted by trained personnel. Decisions must not be based on irrelevant or unreliable information, and candidates must normally have a fair opportunity to explain material discrepancies.

9.2 Online and social media checks

As part of its safeguarding responsibilities, USS may review publicly available online and social-media information for candidates registering for supply work in education. Candidates must be told before checks take place what USS will review, why, at what stage, who may see the outcome and how long relevant records will be retained.

- Checks will be limited to public information and safeguarding or professional-suitability risks relevant to education work.

- USS will not seek access to private accounts, use deception, request passwords or conduct unrestricted trawls.
- Where practicable, the checker will screen out irrelevant special category or personal information before reporting findings to the decision-maker.
- USS will record the search date, sources checked, search terms or identifiers used, outcome and any decision; it will avoid retaining unnecessary screenshots or copies.
- Potential adverse information will be verified as far as reasonably possible and put to the candidate for comment before a decision, unless doing so would create a safeguarding or legal risk.
- Raw irrelevant material will be securely destroyed as soon as practicable. Relevant outcome records will follow the retention schedule.

9.3 DBS and criminal-record information

DBS certificates and criminal-record information are highly sensitive. USS will restrict access, use the information only for authorised suitability and safeguarding purposes, and share only the minimum necessary outcome information. USS will not routinely retain certificate copies. If a copy is temporarily retained for a dispute or exceptional decision, it must be securely stored and destroyed as soon as the purpose ends and normally no later than six months, unless a clearly documented lawful reason requires longer retention. USS may retain a compliance record showing the certificate number, level/type, barred-list information where applicable, issue date, date and method seen, identity of checker, Update Service status/check date and outcome, without reproducing disclosure content unnecessarily.

9.4 Safeguarding information sharing

Data protection law does not prevent necessary and proportionate sharing to safeguard a child or adult at risk. Consent is not always required. Where lawful and necessary, USS may share relevant information with schools, trusts, designated safeguarding leads, local authority designated officers, children's social care, police, DBS, Teaching Regulation Agency, regulators, framework or managed-service partners and professional advisers. Staff must record the purpose, basis, information shared, recipient, date and decision. Urgent safeguarding action must not be delayed while seeking consent or routine advice.

10. Accuracy, fairness and human review

USS will distinguish fact from opinion, source from inference and verified information from allegation. Material decisions about registration, placement, suspension or removal from work will be made by authorised people using relevant evidence. Where automated tools support sourcing, matching, screening or administration, USS will assess bias, accuracy, transparency and data protection risk. USS will not make solely automated decisions producing legal or similarly significant effects unless the law permits this and required safeguards, information and challenge rights are provided.

11. Data sharing and processors

USS shares personal data only where necessary, proportionate and lawful. Recipients may include prospective and current education clients; referees; payroll, pension, umbrella or back-office providers; DBS and identity-check providers; framework or managed-service partners; professional bodies and regulators; government, tax, law-enforcement and safeguarding authorities; insurers, auditors and legal advisers; and IT, CRM, cloud, communications or document-storage suppliers.

- verify the recipient and use a secure transfer method;
- share the minimum data needed and apply need-to-know access;
- put an Article 28-compliant written contract in place before a processor handles personal data;
- perform proportionate due diligence and review processor security and sub-processing;
- use a data-sharing agreement where regular controller-to-controller sharing warrants one; and
- record unusual, high-risk or safeguarding disclosures.

12. International transfers

Personal data must not be transferred or made remotely accessible outside the UK unless an approved legal transfer mechanism and required safeguards are in place. Depending on the destination, this may include UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to EU Standard Contractual Clauses, or another lawful mechanism. USS will complete an appropriate transfer risk assessment where required and provide privacy information about relevant safeguards.

13. Data protection by design and DPIAs

New systems, suppliers, projects or material changes involving personal data must be referred to the Data Protection Lead before implementation. USS will build in data minimisation, access controls, retention, security, transparency and individual rights from the outset. A DPIA must be completed before processing likely to create high risk, and the ICO must be consulted before processing starts if high residual risk cannot be reduced.

14. Information security

- role-based access, unique user accounts, strong passwords and multi-factor authentication where available;
- encryption or appropriately secure methods for storage and transfer, particularly for special category and criminal-record data;
- supported and patched systems, anti-malware protection, firewalls, backups and recovery testing;
- locked storage for paper records, clear desks and secure shredding;
- no storage on personal devices, personal email or unapproved services;

- careful recipient checking, use of BCC where appropriate and password sharing through a separate channel;
- secure remote working, screen locking and protection from unauthorised viewing or discussion;
- prompt removal or adjustment of access when roles change or employment ends; and
- supplier due diligence, confidentiality obligations, training, monitoring and incident response.

15. Retention, deletion and legal holds

USS will retain personal data only for as long as necessary for the purpose, legal or regulatory duties, safeguarding, audit and the establishment, exercise or defence of legal claims. The schedule below is a control framework, not authority to keep every record for the maximum period. A legal, regulatory, insurance, complaint, litigation or safeguarding hold suspends routine deletion until formally released.

Record category	Retention approach
Unsuccessful applicants not joining the active candidate pool	Normally 6 months after the recruitment decision; longer only with a recorded reason or consent for a talent pool.
Registered candidates and workers	During the active relationship; review after 12 months of inactivity and normally erase or minimise after 2 years of inactivity unless legal, safeguarding, contractual or claims reasons justify longer.
Terms, applications, suitability and assignment records required by agency regulations	At least 1 year from creation or after the last supply/introduction, as applicable; longer where another lawful requirement applies.
References and vetting material	Keep only what is needed for suitability, audit and claims. Delete raw intrusive material as soon as practicable; retain a proportionate outcome/audit record.
DBS certificate copy	Do not routinely retain. If exceptionally retained, destroy as soon as the purpose ends and normally within 6 months. Keep a limited check/outcome record.
Online/social-media check material	Delete irrelevant and raw material promptly after assessment. Retain the check log and relevant decision record with the candidate compliance file.
Right-to-work evidence	Duration of employment/engagement plus 2 years after it ends, in line with Home Office requirements.
Payroll, PAYE and tax records	At least the statutory HMRC period; normally 3 years from the end of the relevant tax year, with 6 years used where accounting, contractual or claims requirements apply.
Pension records	For the period required by pensions law; commonly 6 years, with specified opt-out records retained for the statutory shorter period.

Client/supplier contracts and key commercial records	Normally 6 years after termination or the relevant transaction, subject to claims and legal holds.
Marketing suppression records	Minimum information retained as long as needed to ensure the person is not contacted again.
Rights requests, data complaints and breach records	Normally 6 years after closure to demonstrate compliance and manage claims.
Safeguarding, allegation and conduct records	According to applicable safeguarding guidance and the nature/outcome of the matter; may require long-term retention. The Data Protection Lead/DSL must set and record the period case by case.
CCTV or access logs, if used	Normally short periods proportionate to security need, unless required for an incident or investigation.

Deletion must cover live systems and routine repositories. Backup copies may remain until overwritten under the backup cycle, provided they are protected from ordinary use. Paper must be cross-cut shredded or destroyed through an approved confidential-waste service. Where appropriate, USS will record disposal.

16. Individual rights

Subject to legal conditions and exemptions, individuals may have rights to be informed;

- access personal data;
- rectification; erasure;
- restriction; data portability;
- objection, including an absolute right to object to direct marketing;
- and safeguards relating to automated decisions.

Any member of staff receiving a request must forward it to the Data Protection Lead immediately. No special wording is required for a valid request.

USS will verify identity reasonably and proportionately and must not request excessive identification. USS will respond without undue delay and normally within one month. It may extend by up to two further months for complex or numerous requests, telling the person within the first month.

Where clarification is reasonably needed, USS may pause the statutory time limit in accordance with current law, while continuing to handle information that can reasonably be identified.

For access requests, USS will conduct a reasonable and proportionate search and protect third-party information and other exempt material.

A reasonable fee may be charged, or action refused, only where the law permits, including manifestly unfounded or excessive requests. Reasons and complaint rights will be explained.

17. Direct marketing and electronic communications

Marketing must comply with UK GDPR and PECR. USS will identify the correct basis for each audience and channel, provide a clear opt-out, honour objections promptly and retain a minimal suppression record. Purchased or sourced contact data must be lawfully obtained and transparently used. Marketing lists will be reviewed and unnecessary data removed. Service messages about applications, assignments, compliance or contractual matters are not marketing merely because they are sent electronically.

18. Personal data breaches

All actual or suspected breaches - including misdirected emails, lost devices or papers, inappropriate access, malware, unauthorised disclosure, alteration or deletion - must be reported immediately to the Data Protection Lead. Staff must not conceal, independently investigate beyond instructions, or delete evidence.

- contain the incident and recover or protect affected information;
- record what happened, affected people and data, timing, cause, controls and remedial action;
- assess likelihood and severity of risk to people;
- notify the ICO without undue delay and, where feasible, within 72 hours of awareness where risk to individuals is likely;
- inform affected individuals without undue delay where high risk is likely, unless a lawful exception applies;
- notify the relevant controller without undue delay if USS is acting as processor; and document the decision whether or not notification is made and implement lessons learned.

19. Data protection complaints

A person may complain about USS handling of their personal data by emailing info@uniqueschoolsolutions.co.uk. USS will provide an accessible electronic route, acknowledge the complaint within 30 days, investigate appropriately and respond without undue delay. The outcome will explain findings, action taken or proposed, and the right to complain to the Information Commissioner's Office. Complaint records will be kept securely and trends reviewed for improvement.

The ICO can be contacted at www.ico.org.uk or on 0303 123 1113. USS encourages people to contact it first so it has an opportunity to resolve the concern, but this does not remove the right to approach the ICO.

20. Training, audit and monitoring

Personnel will receive data protection and information-security training at induction and refresher training appropriate to risk. Additional training will be provided after significant legal, policy,

Unique School Solutions Ltd
Unit 3, Enterprise Court, Farfield Park, Rotherham, S63 5DB
Telephone: 0114 3392026
Company Registration Number: 10943136

system or process change. USS will monitor compliance through file sampling, access reviews, supplier review, breach and complaint analysis, retention checks and internal or external audit. Failure to follow this policy may result in disciplinary or contractual action and, in serious cases, referral to regulators or law-enforcement bodies.

21. Review and related documents

This policy will be reviewed at least annually and sooner after relevant legal or ICO guidance changes, significant incidents, audit findings or material changes to USS processing. The policy owner will record approval and ensure superseded versions are withdrawn from routine use.

22. Appropriate Policy Document

This section is the USS Appropriate Policy Document for processing special category and criminal offence data where Schedule 1 DPA 2018 requires one. It supplements the Privacy Notice and records of processing.

22.1 Processing and Schedule 1 conditions

USS processes health and disability information, equality information, trade-union information where relevant to employment, safeguarding data and criminal-offence/DBS information for recruitment, employment, worker administration, safeguarding, legal compliance, equality, legal claims and prevention or detection of unlawful acts. USS will record the precise Article 6, Article 9/10 and Schedule 1 conditions in its processing records. Conditions likely to be relevant include

- employment, social security and social protection;
- equality of opportunity or treatment;
- preventing or detecting unlawful acts;
- safeguarding children and individuals at risk;
- regulatory requirements; and legal claims.

22.2 Compliance safeguards

Lawfulness and fairness: document the basis and condition, give transparent information, use relevant evidence and provide human review.

Purpose limitation and minimisation: collect only information needed for a defined recruitment, employment or safeguarding purpose; screen out irrelevant information.

Accuracy: verify material information, record its source/status and allow correction or explanation where appropriate.

Storage limitation: apply section 15, delete raw DBS/online material promptly and use legal holds only where justified.

Security: restrict access to trained authorised staff; protect data in storage and transit; keep disclosure details separate or specially restricted where practical.

Accountability: maintain an APD, processing records, DPIAs where required, decision logs, training and periodic audit.

22.3 Retention of this APD

USS will retain this APD while the relevant processing continues and for at least six months after it ceases. It will review the APD annually and update it when processing, law or guidance changes.