UNIQUE SCHOOL SOLUTIONS

Privacy Notice and Data Protection Policy

For candidates, workers, clients, referees and website users

Document owner	Directors, Unique School Solutions Ltd
Effective date	2 September 2026
Review date	September 2027, or sooner if law or processing changes
Status	Approved policy and public-facing privacy notice

Purpose. This document explains how Unique School Solutions Ltd uses personal information and sets the standards our staff must follow. It is designed to support UK data-protection compliance, safer recruitment in education and clear audit evidence. It does not claim that Unique School Solutions is REC Audited accredited unless and until accreditation is formally awarded.

1. Who we are

Unique School Solutions Ltd ("Unique", "we", "us" or "our") is an education recruitment business providing work-finding and temporary worker services in the UK. For the personal information described in this document, we will usually act as the data controller.

Registered/contact address: Unit 3, Enterprise Court, Farfield Park, Rotherham, S63 5DB
Telephone: 0114 339 2026 | Email: info@uniqueschoolsolutions.co.uk

Data-protection enquiries and complaints may be sent to rebecca@uniqueschoolsolutions.co.uk or to the postal address above.

2. Who this notice covers

This notice applies to candidates, work-seekers, temporary workers, prospective and existing clients, client contacts, referees, suppliers, website visitors and other people whose information we use in connection with our services.

3. Information we collect

Depending on your relationship with us, we may collect:

- identity and contact details, date of birth, address history, photograph and emergency-contact details;
- CV, application, employment and education history, explanations for gaps, qualifications, professional registrations, training and interview notes;
- identity, nationality and right-to-work evidence and check results;
- references, suitability information, disciplinary or safeguarding information, complaints and investigation records;
- DBS and barred-list information where legally permitted, including certificate details and the outcome of checks; we do not routinely retain a copy of a DBS certificate or its disclosure content;
- health, disability and adjustment information, equality-monitoring information and other special-category information where relevant and lawful;
- National Insurance, tax, payroll, pension, bank, timesheet, absence and holiday information;
- publicly available online information generated by proportionate online and public-facing social-media checks;
- communications, call notes, placement history, availability, preferences, performance feedback and compliance records;
- technical and website information such as IP address, device/browser data and cookie information, where applicable.
- Criminal-offence information is not "special-category data" under the UK GDPR, but it is subject to separate enhanced protection. We handle it accordingly.

4. Where information comes from

We obtain information directly from you and, where appropriate, from:

- jobs boards, recruitment platforms, professional networking sites and publicly accessible online sources;
- former employers, referees, schools, academy trusts, nurseries, colleges and other education providers;
- the Disclosure and Barring Service, Teaching Regulation Agency, right-to-work services and other official or professional bodies;
- other recruitment businesses or framework/supply-chain partners where you have engaged with that route;
- our payroll, compliance, IT, communications and software providers;
- events, enquiries, referrals and information supplied by authorised representatives.

Where we obtain your information from elsewhere, we will provide privacy information within the period required by law, unless an exemption applies.

5. Why we use information and our lawful bases

We identify and record the appropriate lawful basis before processing. Consent is not our default basis for necessary recruitment, compliance or safeguarding activity.

Purpose	Typical information	Main Article 6 basis/bases
Registration, matching and work-finding services	Contact, CV, availability, skills and preferences	Contract/pre-contract steps; legitimate interests
Assessing suitability and safer recruitment	Application, interview, references, vetting, online checks and safeguarding information	Legal obligation where applicable; legitimate interests
Placement, contract and worker management	Assignment, attendance, performance, communications and client feedback	Contract; legitimate interests; legal obligation
Right to work, tax, payroll and employment records	Identity, RTW, NI, tax, bank, pension and timesheets	Legal obligation; contract
Protecting children and responding to concerns	Relevant safeguarding, conduct and criminal-offence information	Legal obligation where applicable; legitimate interests; vital interests in an emergency
Business administration, audit and legal claims	CRM records, correspondence, compliance evidence and financial records	Legal obligation; legitimate interests
Relevant vacancy updates and marketing	Contact details, preferences and engagement	Consent where required; otherwise legitimate interests and applicable electronic-marketing rules

6. Special-category and criminal-offence information

Where we use special-category information, we identify both an Article 6 lawful basis and an Article 9 condition. Depending on the purpose, this may include employment and social-protection obligations (Article 9(2)(b)), legal claims (Article 9(2)(f)), or substantial public interest (Article 9(2)(g)) supported by an applicable condition in Schedule 1 to the Data Protection Act 2018, including safeguarding children and individuals at risk where the legal tests are met.

Where we use criminal-offence information, we identify an Article 6 basis and an Article 10/DPA 2018 Schedule 1 condition. This may include employment-related obligations or safeguarding children and individuals at risk, where applicable. Unique maintains an Appropriate Policy Document where the law requires one.

7. Online and social-media checks

Our approach. Because candidates may be placed in roles involving children or vulnerable people, Unique carries out a proportionate online search as part of registration and safer-recruitment due diligence. This is a Unique safeguarding control; KCSIE separately advises schools and colleges to consider online searches on shortlisted candidates.

We will tell candidates about the check before it is undertaken. The check:

- uses search engines and information that is genuinely public, including public-facing professional or social-media content;
- does not involve requesting passwords, attempting to access private accounts, "friending" a candidate, covert methods or intrusive specialist searches;
- is limited to identifying information reasonably relevant to suitability to work in education, safeguarding, professional conduct, serious reputational risk, identity inconsistencies or information requiring clarification;
- does not treat protected characteristics, lawful private-life choices, trade-union activity, political or religious views, or irrelevant personal information as selection criteria;
- is carried out using a consistent search method and recorded on a standard check record;
- should, wherever reasonably practicable, be screened by a trained person who is not the sole decision-maker, with only relevant findings passed to the decision-maker;
- will not normally lead to an adverse decision without identity and accuracy checks, a relevance and proportionality assessment, and an opportunity for the candidate to explain or correct the information.

The usual lawful basis is our legitimate interest in safer recruitment and protecting children, balanced against the candidate's rights. Where a finding contains special-category or criminal-offence information, we will only use it if an additional lawful condition applies. We document the purpose and balancing assessment.

Raw search material, screenshots and irrelevant information must be securely deleted as soon as reasonably practicable after the assessment. We may retain a concise record that the check took place, the outcome, any relevant concern considered, the candidate's response and the decision rationale in accordance with the retention schedule below.

8. Automated decision-making

We do not make solely automated decisions that produce legal or similarly significant effects about candidate suitability. Recruitment and safeguarding decisions involve human review. If this changes, we will provide the information and safeguards required by law.

9. Who we share information with

Where necessary and proportionate, we may share relevant information with:

- schools, academy trusts, nurseries, colleges and other prospective or current clients;
- referees, former employers and professional or qualification-verification bodies;
- payroll, pension, banking/payment, compliance, DBS, right-to-work, IT, CRM, communications and professional-adviser providers;
- framework providers, managed-service providers and other recruitment businesses in the supply chain, including where a placement is delivered through a compliant subcontracting route;
- HMRC, the Home Office, DBS, TRA, regulators, auditors, insurers, courts and law-enforcement bodies where lawful;
- DSLs, LADOs, children's social care, police or other safeguarding bodies where sharing is necessary to protect a child or another person.

We share only what is relevant and necessary, use appropriate security, and put processor or data-sharing terms in place where required. Routine candidate profiles are normally shared with the candidate's knowledge. Consent is not always required for lawful safeguarding, regulatory, crime-prevention or legal disclosures.

10. International transfers

Our services concern UK roles. Some approved technology or service providers may nevertheless process information outside the UK. Where this happens, we use a lawful transfer mechanism, such as UK adequacy regulations, the UK International Data Transfer Agreement/Addendum, or another permitted safeguard, and carry out any required risk assessment. Details may be requested from us, subject to lawful confidentiality restrictions.

11. How long we keep information

We keep information only for as long as needed for its purpose, legal obligations, safeguarding, audit and the establishment or defence of legal claims. The periods below are a summary; a legal hold, active complaint, safeguarding concern or claim may justify longer retention.

Record	Typical retention approach
Work-seeker/recruitment records	While registration is active and at least one year after creation or the last work-finding service, as required by the Conduct Regulations; thereafter reviewed against need and claims risk.
Right-to-work evidence	Duration of employment/engagement and two years after it ends, where the statutory excuse requirements apply.
Payroll, tax, pension, holiday and working-time records	For the applicable statutory period, commonly three to six years depending on the record.

DBS certificate/disclosure	The original is checked and returned. Copies or disclosure content are not routinely retained; if exceptionally retained, no longer than necessary and normally no more than six months. A restricted check/outcome record may be retained longer.
Online-check raw material	Deleted as soon as reasonably practicable after assessment, normally within six months at the latest unless needed for an active concern or claim. A concise audit record/outcome may be kept with recruitment records.
Client, contract, invoice and placement records	Normally six years after the end of the relevant relationship or transaction, subject to legal requirements.
Unsubscribed marketing record	A minimal suppression record may be retained so that we respect the opt-out.

12. Security and confidentiality

We use proportionate technical and organisational measures, including access controls, passwords and multi-factor authentication where appropriate, secure systems, staff training, confidentiality requirements, supplier due diligence, backup and incident-management arrangements. Access is limited to people who need the information for their role. No transmission or storage method is completely risk-free, but we regularly review our controls.

13. Your rights

Subject to the law and any applicable exemptions, you may have the right to:

- be informed and obtain access to your personal information;
- have inaccurate information corrected and incomplete information completed;
- request erasure or restriction in certain circumstances;
- object to processing based on legitimate interests or to direct marketing;
- receive certain information in a portable format;
- withdraw consent at any time where consent is the basis, without affecting earlier lawful processing;
- ask for human intervention where qualifying automated decision-making applies.

To exercise a right, contact us using the details in section 1. We may need to verify your identity. We normally respond within one month, although the law permits an extension in some circumstances.

14. Data-protection complaints

You can complain to us by email or post using the details in section 1. We will provide an accessible route, acknowledge a data-protection complaint within 30 days, make appropriate enquiries without undue delay, keep you informed where appropriate and communicate the outcome without undue delay.

You may also complain to the Information Commissioner's Office (ICO): Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; telephone 0303 123 1113; website https://ico.org.uk/make-a-

complaint/. We would welcome the opportunity to address your concern first, but you do not have to contact us before approaching the ICO.

15. Website links and cookies

Our website may link to external websites that operate under their own privacy practices. This notice does not govern those sites. Information about cookies and choices should be provided through our website cookie notice and consent mechanism.

16. Governance and staff responsibilities

To support accountability and audit readiness, Unique will:

- maintain a record of processing activities or equivalent data map, lawful-basis records and legitimate-interests' assessments;
- maintain an Appropriate Policy Document when required for special-category or criminal-offence processing;
- use documented recruitment, online-check, DBS, retention, breach, rights-request and complaint procedures;
- ensure staff receive appropriate data-protection, confidentiality and safer-recruitment training;
- apply data minimisation, need-to-know access, accuracy checks and secure disposal;
- carry out appropriate due diligence and written contracts for processors and supply-chain partners;
- record significant safeguarding information-sharing decisions, including the rationale for sharing or withholding;
- report and investigate suspected personal-data breaches promptly and notify the ICO and affected people when legally required;
- review this document at least annually and when processing, guidance or law materially changes.

All staff must follow this policy. Concerns or suspected breaches must be escalated immediately to a director and must not be concealed or informally resolved without a record.

17. Changes to this document

We may update this document from time to time. The current version will show its effective date. We will communicate material changes where appropriate.

Appendix A - principal reference framework

This document has been prepared with reference to the UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025, Conduct of Employment Agencies and Employment Businesses Regulations 2003, current ICO recruitment and selection guidance, and Keeping Children Safe in Education 2026. The privacy notice does not replace the operational records, assessments and procedures needed to demonstrate compliance.

ICO, "Pre-employment vetting of candidates": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/recruitment-and-selection/pre-employment-vetting-of-candidates/

ICO, "A guide to lawful basis": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/

ICO, "The Data (Use and Access) Act 2025 - what does it mean for organisations?": https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-what-does-it-mean-for-organisations/

Department for Education, "Keeping children safe in education 2026": https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Document control: Version 3.0 | Effective 2 September 2026 | Next review September 2027

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