



WORKFORCE PRIVACY NOTICE

Employees, candidates, workers, contractors, interns and volunteers

Status	Approved
Effective date	1st September 2026
Last reviewed	August 2026
Next review	August 2027, or earlier if our processing or the law materially changes
Document owner	Data Protection Officer

1. About this notice

Redshift Education takes the privacy of everyone who works for, applies to work for or supports our organisation seriously. This notice explains what personal information we collect about you, why we use it, who we may share it with, how long we keep it and the rights available to you.

It applies to current and former employees, job applicants, workers, agency workers, individual contractors and consultants, interns, work-experience participants and volunteers. Corporate suppliers and other business contacts are covered by our General Privacy Notice.

This notice does not form part of any employment contract, contract for services or volunteer arrangement. It should be read alongside our Group Data Protection Policy, Group Data Retention and Disposal Policy, IT and Acceptable Use Policy, CCTV Policy and other relevant workforce policies.

2. Who is responsible for your information

Redshift Education Ltd, including the schools it operates, is the data controller responsible for the personal information described in this notice. In this notice, “Redshift”, “we”, “us” and “our” mean Redshift Education Ltd and the relevant school or central team.

Redshift Education Ltd is registered in England and Wales under company number 16343353. Its registered office is 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ. Its Information Commissioner's Office registration number is ZB944980.

Our Data Protection Officer oversees compliance across Redshift Education and can be contacted at dpo@redshifteducation.co.uk or at the registered office above.

We process personal information in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, and other applicable law.

3. Personal information we collect

The information we collect depends on your role and relationship with Redshift. It may include:

- identity and contact details, including your name, title, addresses, telephone numbers, personal email address, date of birth, gender, marital or civil-partnership status and dependants;
- emergency-contact and next-of-kin details;
- National Insurance number, tax status, bank details, payroll records, salary, allowances, expenses, pension, benefits and annual-leave information;
- recruitment and suitability information, including applications, CVs, cover letters, interview notes, references, right-to-work documents, identity documents and employment history;
- role and engagement information, including job title, workplace, start and end dates, working hours, contracts, responsibilities and organisational reporting lines;
- qualifications, professional memberships and registrations, training, continuing professional development and mandatory compliance records;
- performance, appraisal, capability, disciplinary, grievance, complaint and investigation information;
- attendance, absence, sickness, family-related leave, flexible-working and workplace-adjustment information;
- safeguarding and suitability information, including DBS and barred-list checks, prohibition or management checks, allegations, referrals and information relevant to working with children;
- communications and records created during your relationship with us, including emails, meeting notes, correspondence and survey responses;
- photographs, audio or video recordings, CCTV footage, access-control records and identification photographs;

- information about your use of Redshift devices, accounts, networks, email, internet, communications and other IT systems, including security and monitoring logs; and
- vehicle, driving, travel, accident, incident, insurance and health-and-safety information where relevant to your role.

4. Special-category and criminal-offence information

Some information receives additional legal protection. Special-category information we may process includes information about racial or ethnic origin, religious or philosophical beliefs, trade-union membership, physical or mental health, disability, sexual orientation and, if ever used to identify a person, biometric or genetic information.

Information about criminal convictions and offences is not special-category information, but it is separately protected. We may process DBS results, barred-list information, prohibition or management checks, allegations and other criminal-offence information where this is necessary and lawful for safer recruitment, safeguarding, suitability, regulatory compliance, legal claims or the protection of pupils and others.

We do not routinely retain copies of DBS certificates. Where a copy is temporarily retained, it is kept only for the period permitted by our Retention Schedule unless a specific lawful reason requires otherwise. We may retain a record that an appropriate check was completed, its date, level and outcome where permitted.

5. How we obtain information

We collect information directly from you through applications, onboarding, forms, meetings, day-to-day communications and your work or activities with Redshift.

We may also obtain information from other sources where relevant, including:

- Cognita Schools Limited or another previous employer, owner, transferor or acquired business, including as part of a TUPE transfer or business acquisition;
- recruitment agencies, referees, former employers and other people you ask to provide information;
- the Disclosure and Barring Service, Teaching Regulation Agency, professional bodies and other checking or regulatory organisations;
- the Home Office, UK Visas and Immigration, HM Revenue & Customs, local authorities and other public bodies;
- occupational-health professionals, healthcare providers, insurers, pension and benefits providers;
- school leaders, managers, colleagues, pupils, parents, volunteers and other witnesses where relevant to an incident, complaint, safeguarding matter or workplace process; and
- our CCTV, access-control, telephone, email, network, device and other IT systems.

If you provide personal information about another person, such as an emergency contact or dependant, please make sure they know that you have given us their information and direct them to this notice where appropriate.

6. Why we use personal information and our lawful bases

We use personal information only where the law permits us to do so. Depending on the purpose, we may rely on taking steps at your request before entering into a contract, performing a contract with you, complying with a legal obligation, protecting vital interests, or pursuing our legitimate interests or those of another person where these are not overridden by your rights. We use consent only where it is appropriate and genuinely optional.

Recruitment, appointment and onboarding

- administering applications, interviews, assessments and recruitment decisions;
- checking identity, qualifications, references, right to work and suitability to work with children;
- determining terms, responsibilities, pay and proposed working arrangements; and
- making reasonable adjustments and preparing for your appointment or engagement.

We rely mainly on pre-contractual steps, legal obligations and our legitimate interests in recruiting suitable people and operating a safe, fair and effective recruitment process.

Managing the working relationship

- administering contracts, working arrangements, personnel records, rotas, attendance, leave and workplace access;
- paying salary, fees and expenses and administering tax, National Insurance, pensions and benefits;
- communicating with you and supporting day-to-day school and business operations;
- providing training, professional development, appraisal, performance and career management;
- managing sickness absence, wellbeing, occupational health, reasonable adjustments and fitness to work; and
- administering grievances, disciplinary and capability procedures, complaints, investigations, suspensions and termination arrangements.

We rely mainly on contract, legal obligations and our legitimate interests in managing our workforce and operating our schools effectively.

Safeguarding, suitability and regulatory compliance

- safeguarding pupils and others and responding to concerns or allegations;
- conducting and recording safer-recruitment and ongoing suitability checks;
- making referrals or disclosures to the DBS, Teaching Regulation Agency, local authority designated officer, Ofsted, Department for Education, police or other appropriate bodies; and
- meeting inspection, education, immigration, employment, tax, equality, health and safety and other legal or regulatory duties.

We rely mainly on legal obligations, substantial public-interest conditions, vital interests and our legitimate interests in protecting children and maintaining a safe and compliant organisation.

Safety, security, monitoring and IT

- protecting pupils, staff, visitors, premises, networks, devices, accounts and information;
- operating CCTV, access control, filtering, monitoring, audit logs and information-security controls;
- preventing and investigating misuse, fraud, security incidents, unlawful activity and breaches of policy; and
- supporting continuity, system administration, audit, backup, recovery and legal or regulatory investigations.

We rely mainly on legal obligations and our legitimate interests in keeping our community, premises, information and systems safe and secure.

Equality, planning and organisational management

- monitoring equality of opportunity and preventing unlawful discrimination;
- workforce planning, budgeting, auditing, reporting and service improvement;
- managing insurance, complaints, legal claims and disputes;
- conducting appropriate staff surveys and wellbeing initiatives; and
- supporting a proposed or completed acquisition, transfer, reorganisation, merger or restructuring.

We rely on legal obligations and our legitimate interests in managing and improving Redshift's operations, establishing and defending legal rights, and planning responsibly for organisational change.

Communications, photographs and school community

- providing internal and operational communications;
- maintaining staff directories, identification and appropriate school displays; and
- using photographs or recordings in school, recruitment, website, prospectus, social-media or other communications where lawful and appropriate.

We generally rely on contract, legal obligation or legitimate interests for necessary operational uses. We will identify optional uses and seek consent where consent is the appropriate basis, particularly for prominent

promotional uses unrelated to your role. You may withdraw consent for future use at any time where we rely on it.

7. How we use sensitive information

Where we process special-category information, we also rely on an additional legal condition. Depending on the circumstances, this may include employment, social-security and social-protection law; safeguarding children and individuals at risk; equality of opportunity; preventing or detecting unlawful acts; health or occupational-health purposes; insurance; legal claims; vital interests; or explicit consent where the processing is genuinely optional.

Where we process criminal-offence information, we do so under an applicable condition in the Data Protection Act 2018, including conditions relevant to employment, safeguarding, regulatory requirements, preventing or detecting unlawful acts, legal claims or consent where legally appropriate. We maintain an appropriate policy document where the law requires one.

8. Monitoring and workplace systems

Redshift may monitor use of its devices, accounts, email, internet, networks, communications and other systems where this is necessary and proportionate for safeguarding, security, compliance, service continuity or investigation purposes. Monitoring may include filtering, audit logs, malware and threat detection, access records, email or file review, and review of websites or services accessed through Redshift systems.

Monitoring is carried out in accordance with our IT and Acceptable Use Policy, Digital Safety Policy and other relevant policies. Access to monitoring information is restricted to authorised individuals. We do not routinely use covert monitoring; any exceptional use would require a specific lawful and proportionate justification and appropriate senior approval.

Monitoring may incidentally reveal private or special-category information. You should therefore use Redshift systems in accordance with our policies and should not assume that activity on organisational systems is completely private.

9. Who we share information with

We share personal information only where there is a lawful and proportionate reason. Depending on the circumstances, recipients may include:

- authorised staff at the relevant school and authorised members of Redshift's central team;
- other Redshift group companies where they provide central services or where sharing is otherwise necessary and lawful;
- HR, recruitment, payroll, pension, benefits and expense providers;
- DBS, background-check, occupational-health, healthcare and training providers;
- IT, cloud-storage, communications, security, CCTV, access-control and support providers;
- banks, insurers, auditors, legal advisers and other professional advisers;
- HM Revenue & Customs, the Home Office, UK Visas and Immigration, the Department for Education, Ofsted, the Teaching Regulation Agency, the Disclosure and Barring Service, local authorities and other regulators or public bodies;
- safeguarding partners, the local authority designated officer, social services, the police, courts and other authorities;
- pension trustees or administrators, trade unions and employee representatives where appropriate; and
- another organisation in connection with a proposed or completed reorganisation, acquisition or transfer of a school or business, subject to appropriate safeguards.

Service providers may process information only for agreed purposes and under appropriate confidentiality, security and data-protection obligations. We do not sell workforce personal information.

10. International transfers

Some service providers may store or access personal information outside the United Kingdom. Where personal information is transferred to a country without UK adequacy regulations, we use an approved transfer mechanism, such as the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, together with additional contractual, organisational or technical safeguards where required.

You may contact the Data Protection Officer for further information about the safeguards relevant to a particular transfer.

11. How long we keep information

We keep personal information only for as long as reasonably necessary for the purpose for which it was collected, including legal, regulatory, safeguarding, accounting, insurance and dispute-resolution requirements. Our Group Data Retention and Disposal Policy and Retention Schedule set the detailed periods. We may retain particular records for longer where a safeguarding matter, complaint, investigation, legal hold or other lawful requirement applies.

Our usual periods include:

- unsuccessful candidate records: normally 12 months after the recruitment decision;
- personnel and engagement records: normally for the employment or engagement and six years afterwards;
- payroll, pension, accounting and tax records: normally six years from the end of the relevant financial or tax year, subject to longer requirements for continuing pension rights or inquiries;
- copies of DBS certificates: normally no longer than six months after the relevant decision unless a specific lawful exception is documented;
- routine CCTV footage: normally 21 days, unless footage is isolated for an incident, safeguarding matter, investigation or claim; and
- routine system and security logs: normally 12 months, unless required for an incident, investigation or legal purpose.

Different or longer periods apply to safeguarding allegations, health and safety, pensions, immigration sponsorship, legal claims and some regulatory records. At the end of the applicable period, information is securely deleted, destroyed or anonymised unless there is a lawful reason to retain it.

12. Security

We use appropriate technical and organisational measures designed to protect personal information against accidental or unlawful loss, alteration, disclosure, access or destruction. These include access controls, role-based permissions, staff training, supplier due diligence, contractual controls, incident-management procedures and appropriate technical safeguards.

Access is limited to people who need the information for their role. Staff, contractors and service providers are subject to confidentiality obligations and must follow our data-protection and information-security requirements.

13. Automated decision-making

We do not currently make recruitment or workforce decisions based solely on automated processing where the decision produces legal or similarly significant effects. Technology may assist with administration, routing, analysis, screening or identifying matters for human review, but a person remains meaningfully involved in significant decisions.

If this changes, we will provide the information required by law and explain the applicable safeguards and rights.

14. If you do not provide information

Some information is required to consider an application, enter into or perform a contract, pay you, assess suitability, safeguard pupils or comply with legal duties. If you do not provide required information, we may be unable to progress an application, appoint or engage you, provide a benefit or fulfil the working arrangement. We will identify voluntary information where this may not be obvious.

15. Your rights

Depending on the circumstances, you may have rights to:

- receive clear information about how your personal information is used;
- request access to your personal information;
- ask us to correct inaccurate or incomplete information;
- ask us to erase information where there is no lawful reason to continue using it;
- ask us to restrict how information is used in certain circumstances;
- object to processing based on legitimate interests or a public task, and object at any time to direct marketing;
- receive certain information in a structured, commonly used and machine-readable format and ask for it to be transferred where data portability applies;
- withdraw consent at any time where we rely on consent, without affecting processing already carried out; and
- rights relating to significant decisions based solely on automated processing, where applicable.

These rights are not absolute and exemptions may apply. We may need information to confirm your identity before responding. You do not normally have to pay a fee, although the law permits a reasonable fee or refusal in limited circumstances, including certain manifestly unfounded or excessive requests.

To exercise a right, contact dpo@redshiftdeducation.co.uk. You do not have to use a particular form for a valid request.

16. Questions and complaints

If you have a question or concern about how we use your personal information, please contact your school or line manager, the central HR team or our Data Protection Officer at dpo@redshiftdeducation.co.uk.

We will facilitate data-protection complaints, acknowledge receipt within 30 days and investigate and respond without undue delay. We may ask for information reasonably needed to clarify the complaint or confirm your identity.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK's data-protection regulator. Current contact details and complaint information are available at <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.

17. Changes to this notice

We review this notice at least annually and whenever there is a material change to our processing, systems or legal obligations. The latest version will be made available internally and on relevant school or Redshift websites. We will use appropriate means to draw significant changes to the attention of affected individuals.