

Privacy and Data Handling Policy

Date of Review	14/09/2026
Next Review Date	14/09/2027
Review Cycle	At least annually
Policy Author	Roger Blundell

Part A - Data Protection Policy

1. Purpose and Scope

educationRnR Ltd is committed to protecting personal information and using it fairly, lawfully and securely.

This policy applies to personal information handled during recruitment, staffing, employment, client management and business administration. It covers candidates, temporary workers, employees, client and supplier contacts, referees, emergency contacts and people who contact us or use our website.

It applies to information held electronically, on paper, in communications and through approved service providers.

Part A sets out our internal responsibilities and controls. Part B explains to individuals how their information is used.

2. Responsibility

Roger Blundell, Director, is the senior person responsible for data protection and the main contact for questions, requests and concerns.

Email: roger@educationRnR.com

Telephone: 01245 969 031

Postal address: Suite 109, Waterhouse Business Centre, 2 Cromar Way, Chelmsford, Essex CM1 2QE.

All staff must follow this policy, complete relevant training and report suspected breaches promptly. Managers must ensure that staff have appropriate access and understand their responsibilities. Anyone processing information on our behalf must be subject to appropriate confidentiality and contractual requirements.

3. Standards for Handling Personal Information

educationRnR will:

- Identify and record a lawful basis before using personal information.
- Explain how information is used through appropriate privacy information.
- Collect only information relevant to a defined business purpose.
- Check accuracy and correct material errors.
- Restrict access and disclosure to those with a legitimate need.
- Keep information only for a justified period.
- Apply appropriate security and dispose of information securely.
- Maintain records demonstrating how these requirements are met.

Personal information must not be reused for an unrelated purpose without assessing the lawful basis and any need to inform the people concerned.

4. Recruitment and Sensitive Information

Recruitment records may contain identity documents, employment histories, references, health information and criminal-record or safeguarding information.

Staff must collect and use sensitive information only where necessary and permitted for the particular role or purpose.

Before processing special-category information, educationRnR must identify an applicable additional condition under data protection law. Criminal-offence information requires separate legal authorisation or an applicable statutory condition.

Where required, educationRnR will maintain an appropriate policy document recording the relevant safeguards and retention arrangements.

Access to sensitive information is restricted. Clients should receive only the information necessary for their recruitment, employment or safeguarding responsibilities. Full identity documents, medical details or criminal-record information must not be routinely circulated with candidate profiles.

5. Secure Systems and Working Practices

Personal information must be stored in approved business systems, including our recruitment systems and controlled SharePoint locations where appropriate.

Staff must:

- Use individual accounts and keep passwords confidential.
- Use multi-factor authentication where available.
- Apply access permissions appropriate to the person's duties.
- Check recipients and sharing permissions before sending information.
- Use secure transfer methods appropriate to the sensitivity of the information.
- Keep devices and software updated and lock unattended devices.
- Store paper records securely and use confidential disposal arrangements.
- Report lost devices, incorrect disclosures and suspicious access promptly.
- Avoid personal email accounts, unapproved storage and unapproved AI tools for business personal information.

Cloud storage may be used where its security, contractual arrangements, access controls and international-transfer implications have been assessed and approved.

Access must be reviewed when responsibilities change and removed promptly when no longer required.

6. Suppliers, Clients and International Transfers

Before appointing a service provider that handles personal information, educationRnR will assess the provider's role, security arrangements, subcontractors and processing locations.

Where a provider acts as our data processor, a written agreement must cover instructions, confidentiality, security, assistance with individual rights and breaches, and the return or deletion of information.

Where clients or other organisations act as separate controllers, information sharing must have a defined purpose and lawful basis.

Information must not be transferred or made accessible outside the UK without assessing whether international-transfer requirements apply and putting the necessary arrangements in place.

7. Retention and Disposal

educationRnR retains personal information in accordance with Appendix A - Records Retention and Disposal Schedule, which forms part of this policy.

The schedule identifies the record type, retention period, starting point and reason for retention. Some periods reflect statutory requirements; others are company-selected periods for recruitment administration, safeguarding accountability or handling claims.

Different documents within the same file may have different retention periods. Retaining a core candidate record does not automatically justify retaining every identity document, medical record or DBS certificate.

Roger Blundell, Director, is responsible for overseeing the schedule. Staff must:

- Record the relevant closure, last-service or employment-end date.
- Review records when their retention period expires.
- Securely delete or anonymise information no longer required.
- Restrict access to records retained solely for legal, regulatory or safeguarding purposes.
- Record any exception, its reason and the next review date.

Routine deletion must be suspended for relevant records where a complaint, safeguarding matter, investigation, legal claim or other preservation obligation remains unresolved. The Director must document the scope and duration of that suspension.

Contractual and accreditation requirements must be checked before disposal. Any different period must have a documented justification; it must not be applied automatically to unrelated information.

Electronic and paper records must be disposed of securely. Information awaiting expiry from backups must remain protected and must not be restored into routine use without reapplying the relevant deletion decisions.

Requests for deletion are assessed individually. We will explain where information must be retained and remove other information where appropriate.

8. Individual Requests and Complaints

Staff must forward any request concerning personal information promptly to Roger Blundell. Requests do not need to use legal terminology or a particular form.

educationRnR will assess the request, verify identity where necessary and respond within the applicable statutory period.

Data protection complaints must be recorded, acknowledged within 30 days, investigated without undue delay and followed by an explanation of the outcome and any corrective action.

9. Personal Data Breaches

A personal data breach may involve loss, unauthorised access, incorrect disclosure, alteration or unavailability of personal information.

Staff must report suspected breaches immediately to Roger Blundell, preserve relevant evidence and assist with containment.

The Director will assess the risks, record the incident and determine the required notifications. Where notification to the ICO is required, it must be made without undue delay and, where feasible, within 72 hours of awareness. Affected individuals must be informed without undue delay where the breach is likely to create a high risk to them.

Where educationRnR acts as a processor, the relevant controller must be notified without undue delay. Contractual notification requirements must also be followed.

10. Training, Monitoring and Review

Staff receive relevant data protection guidance through induction and updates when procedures or responsibilities change.

The Director will review access arrangements, retention practices, incidents, complaints and supplier arrangements proportionately to the risks involved.

New systems and significant changes to processing must be assessed before implementation. A data protection impact assessment must be completed where the proposed processing is likely to create a high risk to individuals.

This policy is reviewed at least annually and following significant changes in law, services, systems or identified risks.

Part B - Privacy Notice

11. Who We Are

educationRnR Ltd provides recruitment and staffing services, including permanent recruitment, temporary and contingent staffing, leadership recruitment and nominated-worker services.

We normally act as the controller of the personal information we use for these activities. This means we decide why and how it is used.

A school, trust or other client may separately control information it receives and uses for its own recruitment or employment purposes. Its own privacy notice will apply to that processing.

For questions or requests, contact Roger Blundell using the details in section 2.

12. Information We Collect

Depending on your relationship with us, we may collect:

Candidates and workers

- Name, contact details, date of birth and identity information.
- CV, employment history, qualifications, professional registrations and references.
- Work preferences, availability, interview notes and assessment information.
- Right-to-work evidence and relevant immigration information.
- Role-appropriate DBS, barred-list, professional prohibition, overseas and safeguarding checks.
- Assignment details, attendance, timesheets, pay, bank, tax and pension information.

- Relevant health or disability information, including reasonable-adjustment needs.
- Complaints, incidents, allegations and information needed to resolve disputes.
- Emergency-contact details.

Employees and applicants for internal roles

- Recruitment and employment records.
- Pay, benefits, leave, training and performance information.
- Information needed for workplace adjustments, health and safety, and employment administration.

Clients, suppliers and referees

- Names, business contact details, roles and correspondence.
- Recruitment requirements, contracts, billing and payment information.
- Reference responses and records of service delivery.

Website users and people contacting us

- Information submitted through enquiries, applications or other forms.
- Relevant technical and security information generated when using our online services.
- Communication preferences.

We do not collect every category for every person. Collection depends on the services involved and the information reasonably required.

13. Where Information Comes From

We may obtain information:

- Directly from you through applications, registration, interviews and communications.
- From clients, employers, referees, professional contacts and authorised representatives.
- From recruitment platforms or job boards on which you have made your details available.
- From relevant public professional profiles, registers and role-appropriate online checks.
- From identity, right-to-work, DBS and other authorised checking services.
- Through records generated during employment, recruitment and assignments.

Where information is obtained from another source, we provide relevant privacy information within the applicable time limit, unless a lawful exception applies.

14. Why We Use Information and Our Lawful Bases

Purpose	Lawful basis normally used
Registering candidates, arranging work and administering agreements with individuals	Taking steps at your request before entering a contract, or performing a contract with you
Searching for suitable candidates, matching people to roles and communicating about relevant opportunities	Legitimate interests in providing recruitment services, or contract where applicable
Managing client and supplier relationships	Legitimate interests in operating our business; contract where the agreement is directly with the individual
Completing legally required checks and employment administration	Legal obligation
Paying workers and administering tax and pensions	Contract and legal obligation
Assessing suitability, obtaining references and conducting proportionate safeguarding checks	Legal obligation where applicable; otherwise legitimate interests, subject to additional safeguards for sensitive information

Managing complaints, incidents, fraud prevention and legal claims	Legitimate interests and legal obligation where applicable
Providing optional marketing communications	Consent where required; otherwise legitimate interests where permitted by the applicable marketing rules
Providing reasonable adjustments and meeting employment-related responsibilities	Legal obligation and the applicable additional condition for health or other special-category information

Our legitimate interests include finding suitable people for roles, maintaining service quality, protecting candidates and clients, securing our systems and managing our business. We assess those interests against the rights and interests of the individuals concerned.

Where consent is required, it is requested separately and can be withdrawn.

Health and other special-category information, and criminal-offence information, are processed only where the relevant additional legal conditions are met. These may include employment and social-protection obligations, legally authorised safeguarding purposes or legal claims, depending on the circumstances. We do not rely on a general registration consent to authorise every type of sensitive check.

15. Providing Information

Some information is necessary to assess suitability, complete required checks, arrange work or meet employment and payment obligations.

If you do not provide necessary information, we may be unable to progress your application, clear you for an assignment or provide the requested service. We will explain which information is required and why.

Optional information is identified as such. Refusing optional marketing consent does not prevent access to our recruitment services.

16. Who We Share Information With

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

- Prospective and actual employers, schools, trusts and other clients.
- Referees and organisations verifying employment, qualifications or professional status.
- DBS and other authorised screening providers, including CareCheck where used.
- Payroll, pension, banking and payment providers.
- Approved IT, recruitment-system, document-storage and communications providers.
- Professional advisers, insurers and auditors.
- HMRC, regulators, safeguarding authorities, law-enforcement bodies and courts where appropriate.
- A prospective purchaser or successor to the business, subject to appropriate confidentiality and data protection safeguards.

Candidate profiles and relevant suitability information may be shared to progress recruitment opportunities. We seek to keep candidates informed about proposed submissions and restrict disclosure to what is appropriate for the role and recruitment stage.

Recipients must have a legitimate reason to receive the information. Sharing with a client does not mean that every document in a candidate file will be disclosed.

17. International Processing

Our use of technology and service providers may involve processing or access outside the UK.

Where this constitutes a restricted international transfer, educationRnR will use an applicable UK adequacy regulation, appropriate contractual safeguards and any required assessment, or another lawful transfer mechanism.

You may contact us for information about the safeguards applicable to your information and how to obtain a copy, subject to necessary redactions.

18. How Long We Keep Information

Our retention periods are set out in Appendix A - Records Retention and Disposal Schedule.

The period depends on the information concerned and our relationship with you. For example, recruitment records, pay records, right-to-work evidence and DBS certificate information have different retention requirements.

When a period expires, we review the information and securely delete or anonymise it unless continued retention is justified. Relevant records may be kept longer where necessary for a legal obligation, safeguarding matter, complaint, investigation or claim.

Information retained solely for these purposes is restricted and is not automatically available for recruitment or marketing.

You can contact Roger Blundell at roger@educationRnR.com to ask which retention period applies to your information or to request deletion.

19. Your Rights

Depending on the circumstances and applicable law, you may have the right to:

- Obtain access to your personal information.
- Correct inaccurate or incomplete information.
- Request deletion.
- Restrict particular uses.
- Object to processing based on legitimate interests.
- Receive certain information in a portable format.
- Withdraw consent where processing relies on consent.
- Obtain the safeguards applicable to significant automated decisions.

You have an absolute right to object to the use of your information for direct marketing.

These rights are subject to applicable conditions and exemptions. Withdrawing consent does not affect the lawfulness of processing undertaken before withdrawal.

We normally respond to rights requests within one month. Where the law permits an extension or adjustment to the response period, we will explain this. Requests are normally free of charge.

20. Automated Tools and Recruitment Decisions

Our policy is that recruitment and clearance decisions receive meaningful review by an authorised person. Technology may assist with organising records, searching, matching or identifying outstanding information.

Before introducing solely automated decisions that have legal or similarly significant effects, educationRnR will assess the applicable requirements, provide suitable information and implement the necessary safeguards, including human intervention where required.

21. Marketing, Website Use and Cookies

You can opt out of marketing by using the unsubscribe option in a message or contacting us. We may retain limited details on a suppression list so that your preference is respected.

Necessary service communications, such as assignment information or compliance reminders, may continue where there is an appropriate reason to send them.

Any non-essential cookies or similar technologies used by our website must be explained through appropriate website information and consent controls where required. Visiting our website does not, by itself, constitute consent to unrelated processing.

Where calls, meetings or interviews are recorded or transcribed, we must inform participants appropriately about the purpose, lawful basis, access and retention arrangements before recording.

22. Questions and Complaints

Please contact:

Roger Blundell, Director

Email: roger@educationRnR.com

Telephone: 01245 969 031

Address: Suite 109, Waterhouse Business Centre, 2 Cromar Way, Chelmsford, Essex CM1 2QE.

We will acknowledge data protection complaints within 30 days, investigate without undue delay and explain the outcome.

You also have the right to complain to the Information Commissioner's Office:

Website: <https://ico.org.uk/make-a-complaint/>

Telephone: 0303 123 1113.

23. Changes to This Notice

We will review this notice when our services, systems or processing arrangements change. Significant changes will be brought to the attention of affected people where appropriate. A change to this notice does not itself provide consent or authorise a new use of personal information.

Appendix A - Records Retention and Disposal Schedule

Schedule owner: Roger Blundell, Director

Review frequency: At least annually, alongside the Data Protection Policy and Privacy Notice.

A1. Applying This Schedule

Statutory minimum means a period required by applicable legislation.

Company retention period means a period adopted by educationRnR for a stated business purpose. It is subject to necessity, proportionality and review.

Guidance-based period reflects relevant official guidance or safeguarding practice.

Where more than one requirement applies to the same record, retain it for the longest applicable, justified period. This does not extend the retention of unrelated documents in the same file.

An **academic year** runs from 1 September to 31 August. “Five complete academic years” means the five academic years following the academic year in which the relevant event occurred. For example, where the last engagement ended on 15 July 2026, five complete academic years end on 31 August 2031.

A2. Recruitment and Candidate Records

Record type	Retention period and starting point	Basis and instructions
Work-seeker records where no placement was made: application, CV, interview notes and required records of work-finding services	12 months after the later of record creation or the last provision of work-finding services.	Statutory minimum for relevant agency records. At expiry, delete unless the person remains actively engaged with the service and continued retention is documented.
Core records for candidates placed by educationRnR: application, employment history, relevant references, qualifications verification, interview notes and placement history	Five complete academic years following the academic year in which the last engagement ended. If later work-finding services are provided, also meet the applicable 12-month minimum.	Company retention period for recruitment accountability and education-sector placement records. Subject to the specific exceptions below.
Hirer records: client requirements, introductions and records of recruitment services	Six years after the end of the relevant client contract or last service, whichever is later.	Company retention period for contractual records. Also meets the applicable agency-record minimum. Retain only relevant business contacts and supporting information.
Signed worker terms, client terms and assignment confirmations	Six years after the relevant agreement or assignment ends.	Company retention period for contractual evidence. Longer periods require a recorded contractual or legal reason, including where an agreement is executed as a deed.
Right-to-work evidence where educationRnR is the employer responsible for the check	Throughout employment and for two years after employment ends.	Home Office recordkeeping requirement. Use the end of employment, rather than the end of an individual assignment.
Other identity and address evidence	Review at completion of verification. Retain copies only where required for the applicable recruitment checks or a documented audit requirement. Where retained as part of the core compliance file, apply its five-academic-year period.	Company retention rule. Avoid duplicate copies; retain a verification record where that is sufficient.
DBS certificates, copies and detailed disclosure information	Only as long as necessary; normally no longer than six months after the recruitment decision.	DBS guidance. Any exceptional extension must be justified and handled in accordance with DBS requirements. This is separate from the check record below.

Limited DBS check record	Five complete academic years following the academic year in which the last engagement ended.	Company retention period. Record permitted administrative details such as check date, certificate reference, check type, position and recruitment decision. Do not reproduce the certificate's criminal-record content.
Detailed health questionnaires or medical information collected for recruitment or adjustments	Review when the decision is completed or adjustment is no longer needed; thereafter at least annually. Delete unnecessary clinical detail.	Necessity-based company rule. Retain only the minimum decision or adjustment record needed for employment, safety or a claim. Do not automatically retain full medical information for the core-file period.

A3. Employment, Pay and Financial Records

Record type	Retention period and starting point	Basis and instructions
Core internal employee records: employment terms, role changes and essential employment history	Six years after employment ends.	Company retention period for employment administration and claims. Sensitive supporting documents require separate review.
Routine appraisals and development assessments	Two years after employment ends.	Company retention period. Relevant evidence may be retained longer for a documented dispute or investigation.
PAYE and payroll records	At least three years from the end of the tax year concerned. Where also needed as minimum-wage evidence, apply the six-year rule below.	Statutory PAYE minimum. Accounting or other applicable requirements may require longer retention of the relevant records.
Minimum-wage evidence: hours, pay, deductions and supporting timesheets	At least six years, beginning with the day on which the pay reference period immediately following the period covered by the records ends.	Statutory minimum-wage requirement.
Statutory maternity, adoption, paternity, shared parental, parental bereavement and neonatal care pay records	At least three years after the relevant tax year, applying the starting point required for the particular statutory payment.	Statutory-payment requirements. Payroll records may need longer retention under other rows.
Sickness absence and sick-pay administration records	Three years from the end of the tax year concerned, subject to longer applicable payroll requirements.	Company period for absence administration; PAYE rules apply to relevant payment records. Detailed medical information is reviewed separately.

Automatic-enrolment pension records	At least six years from creation of the relevant record.	Statutory requirement. The opt-out exception is below.
Pension opt-out notices	At least four years from the date of the notice.	Statutory requirement.
Company accounting records and supporting invoices	Six years from the end of the last company financial year to which they relate.	Statutory requirement, with longer retention where HMRC rules or an unresolved enquiry require it.
VAT records	At least six years from the relevant record date or last entry.	Statutory requirement. Apply any longer period required by a particular VAT scheme.

A4. Safeguarding, Complaints and Other Records

Record type	Retention period and starting point	Basis and instructions
Safeguarding allegations against a worker or employee, other than allegations found malicious or false	Until normal pension age or ten years from the allegation, whichever is later.	Safeguarding-guidance-based period adopted by educationRnR. Preserve relevant records longer where required by an investigation or legal hold.
Allegations found malicious or false	Review and remove from personnel records in accordance with applicable safeguarding guidance, unless the individual consents to retention.	Consider separately whether any restricted organisational record must be preserved for a specific lawful purpose. Do not treat every allegation as subject to automatic ten-year retention.
Routine service complaints and their resolution	Six years after closure.	Company retention period for service accountability and claims. Safeguarding complaints follow the safeguarding rules.
Data protection requests, complaints and breach records	Six years after closure.	Company retention period for accountability. Retain the request, decision and necessary evidence; avoid retaining an entire duplicate candidate file or disclosure bundle without justification.
Marketing preferences and suppression records	For as long as needed to honour the preference while the relevant marketing activity continues; review annually.	Keep only the minimum identifier and preference necessary to prevent unwanted contact.
Routine enquiries that do not become recruitment, employment or client records	12 months after closure.	Company retention period for follow-up and service administration.
Emergency-contact details	While the employment or assignment relationship requires them; delete within three months of its end unless relevant to an incident.	Company retention period. Remove superseded contact information promptly.

A5. Records Requiring a Separate Entry

Before introducing call recording, meeting transcription, automated candidate assessment or new website tracking, educationRnR must document the information collected, purpose, retention period and deletion method.

These records must not automatically inherit the retention period of the candidate or client file.

Any legally required occupational-health surveillance records must also have a separate retention entry appropriate to the exposure and applicable legislation.

A6. Exceptions and Disposal

The Director must authorise and document any exception, including:

- The records affected.
- The reason continued retention is necessary.
- The applicable legal, contractual or safeguarding requirement.
- Access restrictions.
- The next review date.

Once no exception applies, records must be securely destroyed or irreversibly anonymised. Disposal must cover relevant copies held in email, shared folders and approved systems, subject to controlled backup-expiry arrangements.

This schedule replaces inconsistent retention periods in the previous Privacy and Data Handling Policy.