

The ReConnect Programme – Privacy Policy

OWNERSHIP:	The ReConnect Programme
AUTHORISED BY:	Chief Operating Officer
REVIEW:	August 2027

Purpose

This Privacy Policy explains how The ReConnect Programme collects, uses, stores, shares and protects personal information. It also explains the rights of the people whose information we hold. We are committed to handling personal information lawfully, fairly, transparently and securely, with particular care for information about children and young people.

Scope

This policy applies to children and young people, parents and carers, staff, job applicants, workers, volunteers, contractors, referrers, commissioners, professional partners, suppliers, visitors, website users and anyone who contacts or engages with The ReConnect Programme.

This document provides our core privacy information. We may also give shorter or more specific notices at the point information is collected, for example on referral, consent, recruitment, CCTV, website or event forms. Those notices should be read with this policy.

Who We Are and How to Contact Us

The ReConnect Programme Ltd is the data controller responsible for the personal information covered by this policy.

Company number: 16574107

Registered office: Unit 27 Thurston Granary, Station Hill, Thurston, Bury St Edmunds, England, IP31 3QU

Email: admin@reconnect1-1.com

Telephone: 07599 035520

Website: www.reconnect1-1.com

Data protection enquiries should be marked for the attention of the Data Protection Lead and sent using the contact details above. The term Data Protection Lead is used unless ReConnect formally appoints a statutory Data Protection Officer.

POLICY

The Personal Information We Collect

We collect only information that is relevant and proportionate to the purpose for which it is needed. Depending on the relationship with ReConnect, this may include the following.

Children and Young People

name, address, date of birth, contact details, identifiers and emergency contacts
school, local authority, referrer, attendance, timetable, transport and placement information
education history, starting points, attainment, qualifications, work, progress, session records and reports
EHCPs, SEND information, reasonable adjustments, communication needs and professional reports
health, medical, medication, allergy, disability, dietary and accessibility information
safeguarding, social care, looked-after status, risk assessments, incidents, behaviour and welfare information
photographs, video, audio, artwork, portfolios or case studies where there is an appropriate basis
IT accounts, platform activity, access, security and filtering or monitoring records
views, wishes, feedback, complaints and records of communication

Parents, Carers and Other Family Contacts

names, addresses, telephone numbers, email addresses and relationship to the young person
parental responsibility, authority, court or care arrangements where relevant
communication, consent, attendance, meeting, complaint and feedback records
health or personal information voluntarily shared where relevant to supporting the young person

Staff, Applicants, Workers, Volunteers and Contractors

identity, contact, emergency contact, right-to-work and employment information
applications, CVs, interviews, references, qualifications and employment history
DBS and safer-recruitment check information, without routinely retaining DBS certificate copies
contract, pay, tax, pension, benefits, bank, attendance, leave and working-time records
training, supervision, performance, conduct, grievance, capability and disciplinary information
health, disability, absence, occupational-health, accident and reasonable-adjustment information
IT, email, system-access, security, filtering and monitoring records
photographs, biography, communications and professional profile information where appropriate

Referrers, Commissioners and Professional Partners

names, roles, organisations and professional contact details

referral, placement, funding, invoicing, review, safeguarding and contractual communications
records of decisions, meetings, reports, advice, complaints and quality assurance

Website Users, Enquirers, Visitors and Suppliers

contact details and the content of enquiries, forms, referrals or applications
website technical data, such as IP address, browser, device, pages visited and cookies where used
visitor records, access information and CCTV images where applicable
supplier contacts, contracts, payment, banking, insurance and due-diligence information
marketing preferences and records of consent or objection

Special Category and Criminal Offence Information

Some information requires additional protection. This includes health, disability, race or ethnicity, religion, sexual orientation, biometric information used for identification, trade union membership and other special category data. Safeguarding records may also contain highly sensitive information. Criminal offence information includes convictions, cautions, allegations and DBS check information.

We process this information only where we have both an Article 6 lawful basis and, where required, an appropriate Article 9 condition or Data Protection Act 2018 Schedule 1 condition. Criminal offence information is processed under Article 10 and the Data Protection Act 2018. We maintain an Appropriate Policy Document where required.

How We Obtain Personal Information

We may obtain information:

directly from the individual, young person, parent, carer or family member
from a commissioning school, local authority, social worker, virtual school, health service, youth justice service or other referrer
from previous or current education providers and awarding organisations
from safeguarding partners, police, courts, regulators or professional advisers
from job applicants, referees, former employers, recruitment agencies and official checking services
from our websites, referral forms, systems, devices, CCTV, online platforms and service providers
from publicly available sources where this is relevant, necessary and lawful

Where information is obtained from another source, we will provide privacy information within the period required by law unless an exemption applies or the person already has the information.

Why We Use Personal Information

We use personal information to:

receive, assess and respond to referrals and decide whether ReConnect can meet need
 plan, deliver, monitor, review and evidence education, support, qualifications and placements
 safeguard young people, manage risk, respond to emergencies and cooperate with safeguarding partners
 record attendance, absence, transport, incidents, progress, outcomes and transitions
 make reasonable adjustments and support medical, SEND, communication and accessibility needs
 communicate with young people, families, commissioners, professionals and emergency contacts
 recruit, employ, train, supervise, support and pay staff and workers
 manage contracts, suppliers, insurance, finance, accounts, funding and legal claims
 operate secure premises, websites, IT systems and online learning platforms
 respond to enquiries, rights requests, feedback and complaints
 evaluate quality, demonstrate impact, improve services and meet commissioner requirements
 publish approved photographs, stories or promotional material where a suitable lawful basis applies
 comply with legal, regulatory, safeguarding, health and safety, tax, employment and insurance requirements

Our Lawful Bases

We identify and document the appropriate lawful basis before processing. The basis depends on the purpose and relationship.

Lawful basis	How it may apply
Contract	To take steps before, enter into or perform placement, employment, supplier or service contracts.
Legal obligation	To meet applicable employment, tax, health and safety, safeguarding, regulatory or record-keeping duties.
Vital interests	To protect someone's life or physical safety in an emergency where another basis is not suitable.
Legitimate interests	For proportionate administration, service delivery, security, quality assurance, communication, debt recovery and organisational management, balanced against individual rights.
Consent	For optional uses where genuine choice is possible, such as certain photographs, publicity or electronic marketing. Consent may be withdrawn without affecting earlier lawful processing.

We do not rely on consent where processing is necessary for safeguarding, core placement delivery, legal obligations or another more appropriate basis. Refusing or withdrawing optional consent will not affect access to the core service.

Special Category Conditions

Where we process special category information, the additional condition may include employment and social

protection law, vital interests, legal claims, substantial public interest, safeguarding of children and individuals at risk, equality monitoring, or health and social care. The exact condition is recorded in our Record of Processing Activities and Appropriate Policy Document where required.

Sharing Personal Information

We share personal information only when there is a lawful basis, the sharing is necessary and proportionate, and appropriate security or contractual arrangements are in place. Recipients may include:

- commissioning schools, colleges, local authorities and virtual schools
- parents, carers and persons with lawful responsibility or authority
- social care, police, safeguarding partnerships, health services and emergency services
- education, SEND, therapy, careers, training, work-experience and awarding organisations
- transport providers where information is required for safe travel
- payroll, pension, banking, insurance, occupational-health and professional advisers
- IT, cloud, website, communications, safeguarding, MIS and learning-platform providers acting as processors
- HM Revenue and Customs, courts, regulators, the Information Commissioner's Office and other bodies where legally required
- prospective purchasers or advisers if the organisation changes ownership, subject to appropriate safeguards

Information may be shared without consent where this is necessary for safeguarding, preventing or detecting crime, complying with law, protecting vital interests or another lawful purpose. We do not sell personal information.

Commissioner and Controller Relationships

For placements, ReConnect and the commissioning school or local authority will usually be separate data controllers for their respective functions. Each organisation is responsible for its own lawful processing, transparency and rights handling. Where ReConnect acts as a processor for a specific activity, a written contract meeting Article 28 requirements will be in place.

International Transfers

Some technology or support providers may process information outside the United Kingdom. Before making a restricted transfer, we check the location, purpose and risks and use an appropriate legal safeguard, such as UK adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to approved Standard Contractual Clauses. We also apply proportionate technical and organisational protections.

How We Protect Personal Information

Our controls include:

role-based access and access reviews
strong passwords, multi-factor authentication and managed accounts
encryption, secure transfer and protected devices where appropriate
staff confidentiality, training, supervision and disciplinary controls
secure storage, clear-desk practices and confidential disposal
backups, logging, monitoring, patching and incident response
processor due diligence and contracts

Data Protection Impact Assessments for processing likely to create a high risk

No system can be guaranteed completely secure. Any suspected loss, unauthorised access, disclosure or misuse must be reported immediately under the Data Breach Procedure. Where required, we will notify the Information Commissioner's Office and affected individuals within the applicable legal timeframes.

How Long We Keep Information

We keep information only for as long as needed for the purpose, legal or contractual requirements, safeguarding, insurance and the establishment or defence of claims. Our Records Retention Schedule contains the detailed periods. The following are the normal starting points and may be extended where a safeguarding, legal, investigation or litigation hold applies.

Record category	Normal retention approach
Young person placement and education records	Normally seven years after the placement ends, unless a different commissioner, safeguarding or legal requirement applies.
Safeguarding and child protection records	Retained and transferred in accordance with safeguarding requirements, case circumstances and the Records Retention Schedule.
Accident, incident, medical and risk records	According to the nature of the record, limitation periods, safeguarding need, age of the young person and insurance requirements.
Successful staff records	Normally six years after employment or engagement ends, with specific records kept for longer where law, safeguarding or pension requirements apply.
Unsuccessful applicant records	Normally six months after the recruitment decision, unless longer retention is justified and explained.
Finance, tax and transaction records	Normally six years after the relevant financial year or transaction, subject to applicable requirements.
CCTV	Normally retained for a short period appropriate to the security purpose, unless footage is preserved for an incident, investigation or legal claim.
Website enquiries and marketing preferences	For as long as needed to respond and manage the relationship, with suppression records retained where needed to respect objections.

When information is no longer required, it is securely deleted, anonymised or destroyed.

Your Data Protection Rights

Depending on the circumstances and lawful basis, individuals may have the following rights:

- to be informed about how personal information is used
- to request access to personal information
- to ask for inaccurate or incomplete information to be corrected
- to request deletion where the right to erasure applies
- to request restriction of processing
- to object to processing based on legitimate interests or to direct marketing
- to receive certain information in a portable format where data portability applies
- to withdraw consent at any time where processing is based on consent
- not to be subject to a solely automated decision with legal or similarly significant effects, except where lawful safeguards apply
- to complain to the Information Commissioner's Office

These rights are not all absolute. We may need to verify identity and authority and may withhold information where a lawful exemption applies, including where disclosure would affect another person's rights, safeguarding, legal privilege or an investigation. We normally respond within one month and will explain any lawful extension, refusal or restriction.

Children's Information and Requests

Children and young people have their own data protection rights. We provide information in language and formats suited to their age, understanding and communication needs. A parent or carer does not automatically exercise a child's rights. We consider the young person's competence, best interests, parental responsibility, the nature of the information and any safeguarding concerns. We may respond directly to a competent young person or involve an appropriate adult where necessary.

Automated Decision-Making

ReConnect does not normally make decisions about individuals based solely on automated processing where the decision produces legal or similarly significant effects. If this changes, we will provide specific information about the logic, significance, consequences and safeguards before the processing begins.

Photographs, Portfolios and Publicity

Photographs, recordings, artwork, case studies and portfolio material will be used only for a clear and recorded purpose. Identifiable publicity or social-media use will normally be optional and based on valid consent or another clearly explained lawful basis. Safeguarding, placement restrictions and the young person's wishes will be considered even where an adult has given consent. Consent can be changed or withdrawn for future use, although material already lawfully printed or published may not always be fully retrievable.

Website, Cookies and Electronic Communications

Our website may use cookies and similar technologies. Strictly necessary technologies may operate without consent where the legal exception applies. Non-essential analytics, advertising or similar technologies will be used only after valid consent where required. Current details, purposes, providers and durations should be provided through the website Cookie Notice and consent controls.

Electronic marketing will be sent only where permitted by data protection law and the Privacy and Electronic Communications Regulations. Every marketing message will provide a clear way to opt out. Operational messages about a placement, contract, safeguarding or service are not marketing.

Concerns and Complaints

If you have a concern about how we use personal information, contact the Data Protection Lead at admin@reconnect1-1.com or write to the registered office. We will investigate and respond as promptly as possible.

You also have the right to complain to the Information Commissioner's Office. The ICO recommends contacting the organisation first so that it has an opportunity to resolve the concern.

Information Commissioner's Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 0303 123 1113

Website: www.ico.org.uk

Changes to This Policy

We will review this policy at least annually and whenever our processing, services, technology or legal obligations change. Material changes will be communicated through an appropriate route, which may include our website, direct communication or a replacement privacy notice.

Appendix A: Privacy Information for Young People

This section gives a shorter explanation for young people. Staff can provide it in another format or explain it with you.

What Information Do We Keep?

We keep information that helps us support you safely and plan your time at ReConnect. This can include your name, contact details, school, timetable, attendance, work, progress, EHCP, health needs, support needs, risks and what you tell us about your experience.

Why Do We Need It?

We use it to plan activities, support your learning and wellbeing, keep you and others safe, record your progress, communicate with the people responsible for your placement and help with your next steps.

Who Might We Tell?

We only share information when there is a proper reason. This may include your parent or carer, school, local authority, social worker, health professional or another person helping to keep you safe. We may need to share a concern even if you ask us not to, but we will normally explain what is happening when it is safe to do so.

Can I See or Correct My Information?

Yes. You can ask what information we hold about you and tell us if something is wrong. Some information may need to be withheld to protect you or another person, or because the law allows this. We will explain the decision.

What About Photos?

We will ask before using identifiable photos or stories for optional publicity. You can tell us if you are uncomfortable, even if an adult has agreed. Saying no will not affect your place at ReConnect.

Who Can Help Me?

Speak to any trusted member of staff or contact the Data Protection Lead through admin@reconnect1-1.com or 07599 035520. You can ask a parent, carer, advocate or another trusted adult to help you.

Appendix B: Legal and Organisational Framework

UK General Data Protection Regulation

Data Protection Act 2018

Data (Use and Access) Act 2025

Privacy and Electronic Communications Regulations 2003

Children and Families Act 2014 and relevant education and safeguarding requirements

Human Rights Act 1998

ICO guidance on transparency, children's information, data sharing, security and individual rights

ReConnect Data Protection Policy, Records Retention Schedule, Data Breach Procedure, Information Security Policy, Safeguarding and Child Protection Policy, CCTV Policy and Cookie Notice

Policy Context

AP context (non-school AP): The ReConnect Programme operates as a non-school Alternative Provision (AP). We process information to assess referrals, deliver agreed placements, safeguard young people, monitor attendance and progress, communicate with families and commissioners, manage staff and meet organisational obligations. The ReConnect Programme is normally a separate data controller for its own operations and shares information controller-to-controller with commissioning schools, local authorities and safeguarding partners under documented arrangements.

VERSION CONTROL

Version	Date	Change Summary	Author/Reviewer	Approved by:
1	28/08/2026	policy	Naomi Hamer	Director