

Replenish Learning



Information Governance and Data Protection Policy

Policy Version:	2.0
Date of Issue:	September 2026
Review Date:	September 2027
Approved by:	AK (Director)

1 Purpose and scope

Replenish Learning protects the personal information entrusted to us by children, families, staff and partners. This policy sets out how we collect, use, share, secure and dispose of information, and how people can exercise their rights or raise concerns.

It applies to employees, directors, volunteers, contractors and anyone handling information on our behalf. It covers paper files, daily logs, referral documents, EHCP information, therapeutic records, emails, photographs, recordings, cloud systems and information used during transport, outreach and community activities.

Replenish Learning operates a therapeutic, intervention-led alternative provision supporting engagement, wellbeing and readiness to access education. Placements supplement the arrangements made by the commissioning school or local authority. This policy does not confer school registration or transfer a commissioner's education responsibilities to Replenish Learning.

2 Legal framework and guidance

Our principal data protection framework is the UK General Data Protection Regulation and the Data Protection Act 2018, as amended, including by the Data (Use and Access) Act 2025. We also apply the Privacy and Electronic Communications (EC Directive) Regulations 2003 where relevant to electronic marketing and website technologies, and the Data Protection (Charges and Information) Regulations 2018 where a data protection fee is payable.

Safeguarding decisions take account of the Children Acts 1989 and 2004, including the information sharing duty in section 16LA where applicable, Working Together to Safeguard Children 2026 and the September 2026 statutory guidance Information sharing to safeguard children and young people. We follow relevant local safeguarding partnership procedures and adopt relevant Keeping Children Safe in Education 2026 standards for our work with children. Its statutory application depends on the provider's legal status.

We use current ICO guidance, including guidance on sharing children's information, sensitive data, accountability, subject access and complaints. DfE data protection guidance informs suitable practice, with adaptations for alternative provision.

The Freedom of Information Act 2000 and school-specific education record regulations do not automatically apply to us merely because placements are publicly funded. We assess any applicable duty and assist commissioners with lawful requests. The Protection of Freedoms Act 2012 school and college biometric provisions are applied where within scope. If our status or service changes, the Directors will review these requirements before the change takes effect.

3 Accountability and responsibilities

Replenish Learning is responsible as controller for processing where it determines the purposes and means. The responsible legal entity, address and contact details must be identified in our privacy notices and commissioning agreements. Schools, local authorities and therapeutic professionals may be separate controllers. We do not assume that a commissioning relationship makes us a processor; roles are assessed for each activity.

The Directors retain overall accountability, approve resources and oversee compliance. The Data Protection Lead coordinates requests, complaints, breach response, staff training, retention reviews and processing records. Atique Khan is the named Lead. Staff must report concerns promptly; they must not wait for management approval before taking necessary emergency safeguarding action.

The DSL coordinates safeguarding disclosure decisions and secure child protection transfers. Managers authorise access according to duties. Everyone must use approved systems, maintain accurate records and report errors, losses or inappropriate disclosures immediately.

We assess and record whether Article 37 requires a formal Data Protection Officer, including whether our core activities involve large-scale sensitive data processing or large-scale regular and systematic monitoring. A Data Protection Lead is not automatically a statutory DPO. If required or formally appointed, the DPO must have appropriate expertise, independence, resources and direct access to the Directors, without conflicting decision-making responsibilities. The appointment and contact details will be documented and notified to the ICO as required.

We maintain a record of processing activities, an information asset and supplier register, records of lawful bases, sharing decisions, requests, complaints, breaches and secure disposal. We assess the ICO fee requirement and maintain registration and payment where required. Small staff numbers do not remove record-keeping duties for our regular processing of sensitive information.

4 Data protection principles

We process information lawfully, fairly and transparently; use it for specified purposes; collect only what is necessary; keep it accurate; retain it only while justified; protect its confidentiality, integrity and availability; and demonstrate accountability for these principles.

Pseudonymised information remains personal data where someone can be identified. Anonymous information is used for evaluation only where identification is no longer reasonably possible. Records distinguish observation, the child's words, professional opinion and information reported by others.

5 Information we use and lawful bases

We use necessary information for referrals and placement planning, attendance and safe transport, support and intervention, safeguarding, progress reporting, communication, staff recruitment and employment, payments and organisational administration. Information about disability or SEND is collected to support the child, not to label or disadvantage them.

For each purpose we document an Article 6 lawful basis before processing. Contract applies only where necessary for a contract with the individual, or their requested pre-contract steps. A school or LA commissioning contract does not automatically provide that basis for processing a child's information. Legal obligation requires an identifiable legal duty, not merely a contractual requirement.

Legitimate interests requires necessity and a documented balancing assessment, with particular weight given to children's interests. Where appropriate, the recognised legitimate interests basis introduced by the 2025 Act may apply, but only within its statutory conditions. Public task is used only where the task or authority has a basis in law; public funding alone is insufficient. Vital interests may apply in a genuine life-threatening emergency.

Consent, where used, must be freely given, specific, informed, unambiguous and withdrawable without inappropriate disadvantage. We keep evidence and explain withdrawal. Explicit consent is used where the relevant sensitive data condition requires it. Permission to participate in an activity is distinct from GDPR consent. Consent is not our default basis for essential safeguarding or employment processing.

6 Sensitive information and criminal offence data

Health and disability information, ethnicity, religion and other Article 9 categories require both an Article 6 basis and an Article 9 condition. A safeguarding record may contain special category information or criminal offence information; its content determines the rules.

For safeguarding without consent, where the legal conditions are met, we may rely on Article 9(2)(g) and DPA 2018 Schedule 1 Part 2 paragraph 18. Necessity, substantial public interest and the paragraph's consent-related conditions must be assessed and recorded. For employment health information, Article 9(2)(b) and Schedule 1 Part 1 paragraph 1 may apply. Article 9(2)(h) is used for health or social care only where the legal and professional confidentiality requirements are satisfied. These examples do not authorise every therapeutic or SEND activity automatically.

Criminal convictions, alleged offences, DBS information and related measures are handled under Article 10 and the relevant DPA 2018 authorisation, in addition to an Article 6 basis. Access is restricted to those who need it. Staff must not obtain criminal records by requiring someone to make a subject access request.

Before relying on a condition requiring an Appropriate Policy Document, the Lead must complete and maintain Appendix C with the actual purpose, condition, categories, safeguards and retention arrangements. Consent, confidentiality agreements and general safeguarding wording do not replace the required legal conditions.

7 Privacy notices and confidentiality

We provide separate, accessible notices for children and families, staff and applicants, and other relevant groups. Notices explain the controller, purposes, bases, sensitive data conditions where relevant, sources, recipients,

transfers, retention, rights, complaints and any significant automated decisions. When data comes from a commissioner or another source, we provide the required information within the applicable Article 14 deadline unless a documented exemption applies.

Children receive explanations suited to their communication needs. Staff explain the limits of confidentiality and never promise to keep information secret where sharing is necessary to safeguard someone. Families are told about routine commissioner reporting and therapeutic confidentiality arrangements. We do not routinely circulate full therapy notes where a proportionate summary meets the purpose.

8 Sharing information and safeguarding

We share only relevant, necessary and proportionate information with authorised recipients, including commissioning schools and local authorities, children's social care, police, health services and therapeutic professionals. A contract or recipient's request alone does not establish a lawful disclosure.

Staff must act promptly when a child may be at risk. Lack of consent must not delay a justified safeguarding disclosure. In an emergency contact the appropriate emergency service, then inform the DSL. The statutory information sharing duty is assessed within its legal scope; it is not a blanket authority to disclose entire files.

For non-emergency disclosures, verify identity and authority, record the purpose, lawful basis and additional sensitive data conditions, share the minimum necessary through a secure route, and record what was shared, when, with whom and why. Be open with children and families unless doing so is unsafe, prejudices protection or is otherwise lawfully restricted. Record reasons for a decision not to share as well.

At placement transitions or closure, agree responsibility with the commissioner and receiving setting. Transfer relevant safeguarding information separately and securely, confirm receipt and record the handover. Retaining our own record must be justified; sending a copy does not automatically require us to retain every duplicate indefinitely.

9 Security and working away from the provision

Access is limited by role and reviewed when responsibilities change. Leavers' access is removed promptly. Use individual accounts, strong passwords, multi-factor authentication where available, suitable encryption, updates, malware protection and tested backups. Secure paper files and devices; protect screens and discussions from unauthorised viewing.

Approved cloud storage, including any organisational Google Drive use, must have managed permissions, restricted sharing, supplier checks and suitable contracts. Sensitive files must not be made public through links. Check recipients and attachments before sending; use secure sharing or encryption for sensitive documents and send passwords separately where appropriate.

During transport, outreach and activities, take only necessary information, secure it and return it to approved storage promptly. Do not leave identifiable records or unlocked devices visible in vehicles. Personal email, personal cloud storage and unapproved messaging or AI services must not be used for identifiable provision information. Lost paper notes and misdirected messages are potential breaches. Approved device use must comply with our staff phone and safe use of AI policies.

10 Suppliers and international transfers

Before engaging a supplier, determine whether it is a processor, separate controller or joint controller and record the arrangement. Processor contracts must meet Article 28, including instructions, confidentiality, security, subprocessors, rights assistance, breach assistance, deletion or return and audit arrangements. Independent therapeutic controllers require clear sharing and confidentiality arrangements rather than being labelled processors automatically.

Assess overseas hosting and remote access as well as the supplier's UK address. Restricted international transfers require a valid adequacy route or another lawful mechanism, such as the UK International Data Transfer Agreement or UK Addendum, with the required transfer assessment and supplementary safeguards. The Lead records the mechanism and checks onward transfers before use.

11 Individual rights and subject access

People have rights to information, access, correction, erasure, restriction, objection and portability where applicable, and safeguards concerning significant solely automated decisions. Rights depend on the processing basis and legal exceptions; records necessary for safeguarding are not automatically erased on request.

Staff must pass verbal, written or electronic requests to the Lead immediately and record the date received. No special form or legal terminology is required. Requests are normally free and answered without undue delay within one month. Necessary identity and authority checks must be proportionate and requested promptly. An extension of up to two further months may be used for complexity or multiple requests, with reasons notified within the initial month.

We undertake reasonable and proportionate searches and supply accessible information securely. If clarification is reasonably required, the response clock may be paused under the amended rules; record the dates and explain the effect. Do not use clarification to force a narrower request or create unnecessary delay. Assess third-party information and statutory exemptions individually. Explain any lawful refusal or restriction and rights to complain to the ICO and seek a judicial remedy.

The child's personal data rights belong to the child. Assess understanding and maturity rather than applying a fixed age rule in England. Verify a representative's authority; where a competent child authorises a parent, retain evidence. Where the child cannot exercise the right, assess parental responsibility and the child's best interests, including confidentiality and safeguarding risks. SEND does not automatically remove a child's competence.

12 Complaints about personal information

Anyone can raise a data protection complaint verbally, in writing or by email to the Lead using the contact route in section 17. A special form is not required and staff will assist children and people who need accessible communication. If the complaint concerns the Lead, another Director or a suitably independent reviewer will handle it.

We acknowledge complaints within 30 days of receipt, make appropriate enquiries without undue delay, keep the person informed and communicate the outcome and any corrective action without undue delay. Record dates, evidence, decisions and actions. Thirty days is the acknowledgment deadline, not a universal deadline for completing every investigation. Explain the right to complain to the ICO and provide its complaints details.

13 Retention and secure disposal

Appendix A sets our default periods and review triggers. These are provision retention decisions or identified legal requirements, not a claim that every school retention rule applies to us. The Lead reviews the schedule annually against commissioning requirements, safeguarding guidance, professional duties, insurance and legal limitation periods.

Hold relevant records where needed for an ongoing safeguarding matter, investigation, complaint, claim, court order or preservation notice; document the reason, access controls and review date. On expiry, delete or securely destroy information unless continued retention is justified. Record disposal authorisation and use approved confidential destruction. Apply deletion to working copies and supplier systems, and manage backup expiry so deleted information is not routinely restored into live use.

14 Higher risk activities and new systems

Apply data protection by design and default when changing referral forms, monitoring, apps, transport arrangements or therapies. Screen changes for risk and conduct a DPIA before processing likely to present high risk, including relevant uses of sensitive children's information, surveillance, biometrics or AI. Consult the ICO before proceeding if high residual risk cannot be mitigated.

Photographs and videos need a specified purpose, lawful basis, notice, controlled access and deletion rules. Separate publicity permissions from essential records; refusal of optional publicity must not affect support. CCTV, if introduced, requires a documented purpose, proportionality assessment, notices and restricted retention and access.

Biometric recognition must not be introduced without the Lead's legal and risk assessment. If school or college provisions apply, notify parents as required, obtain the required written consent, honour relevant parental

objections and the child's objection even where a parent consents, and provide reasonable alternatives. Article 9 conditions and DPIA requirements also apply where relevant.

Do not introduce solely automated decisions with legal or similarly significant effects without legal assessment under the amended UK GDPR. Provide required information and safeguards, including representations, human intervention and challenge. Additional restrictions apply to special category data. Children's access to placements or support must not be determined by an unassessed automated tool.

Website cookies and other storage or access technologies must meet PECR, including consent where required and the conditions of any exemption relied on. Electronic marketing requires an assessed lawful route, appropriate consent where required and a clear opt-out. The children's code is assessed if we offer an online service likely to be accessed by children and within its scope.

15 Personal data breaches

All suspected confidentiality, integrity or availability breaches must be reported immediately to the Lead, or to another senior manager if unavailable. Appendix B governs containment, risk assessment, notifications and learning. Safeguarding concerns must also be referred to the DSL promptly.

16 Training and review

Staff receive induction and regular refresher training covering safe recording, sharing, phishing, requests and breach reporting. Directors review compliance at least annually and after significant incidents, legal changes or changes to our provider status. Approval and implementation actions are recorded; no approval date is assumed merely because a revised document has been prepared.

17 Contacts

Data Protection Lead: Atique Khan, Business Manager. Email: a.kahn@replenishlearning.co.uk. Requests, complaints and data protection concerns can be sent to this address or raised directly with the provision. Website: www.replenishlearning.co.uk.

ICO: ico.org.uk/make-a-complaint/ | Telephone 0303 123 1113. People may approach the ICO about their information rights. Emergencies and immediate child protection concerns must use the safeguarding or emergency reporting route.

Appendix A Retention schedule

These periods are defaults subject to documented necessity, applicable duties and legal holds. Retain only the categories needed; not all documents in a folder require the same period.

Record category	Default period or trigger	Reason and qualifications
Child protection records	Until the child's 25th birthday; child sexual abuse records until age 75, subject to current guidance and preservation requirements.	Adopted safeguarding retention benchmarks, transfers, duplicates and any longer justified retention.
Placement and intervention records	Core referral, attendance, plans and outcome evidence: normally 6 years after placement ends. Review sensitive clinical records separately.	Provision accountability and possible child protection concerns; avoid unnecessary duplicates and escalate relevant issues to safeguarding or injury.
Accident and injury records	Child injury records: normally until age 21, or longer where justified by severity, safeguarding, insurer requirements or claims. Adult accident records: normally at least 3 years from the last entry.	Assess applicable reporting law and limit retention periods. Do not apply one period to all records.
Staff core employment records	Normally 6 years after employment ends.	Keep necessary contract and employment records; assess pensions, statutory payroll and other specialist categories separately.

Record category	Default period or trigger	Reason and qualifications
Safeguarding allegations against staff	Relevant substantiated, unsubstantiated or unfounded allegations: normal pension age or 10 years after allegation, whichever later.	Apply current safeguarding guidance. For malicious allegations are normally removed unless another evidenced lawful reason requires retention.
Unsuccessful applications	Normally 6 months after recruitment decision.	Recruitment challenge period. Talent pool requires a separate justified purpose and retention.
DBS certificates	Normally do not retain copies. If exceptionally necessary, generally no longer than 6 months after the recruitment decision.	Retain permitted check metadata and data for evidence instead; restrict certificate access and securely destroy copies.
Financial and tax records	Normally 6 years from the end of the relevant accounting period for company records; apply specific longer duties or shorter payroll requirements where appropriate.	Tax and accounting evidence. The trigger is simply the date an invoice was created.
Complaints, rights requests and breach logs	Normally 6 years after closure; review sensitive supporting material for earlier disposal.	Accountability and potential claims; child protection matters follow the safeguarding schedule.
Optional publicity images	Review annually; remove when the stated purpose ends or applicable consent is withdrawn.	Operational assessment images may include the placement schedule.
CCTV and visitor records	If CCTV is introduced, normally up to 30 days; visitor logs normally 12 months.	Adopted defaults requiring documented retention; preserve relevant extracts for a recorded claim.
Temporary working copies	Delete promptly after verified entry or transfer to the approved record.	Avoid multiple uncontrolled copies; retain receipts as necessary evidence.

Appendix B Data breach response procedure

1. Report immediately. Record when the incident occurred, when it was discovered and when Replenish Learning became aware of a personal data breach. Include systems, data, people and possible recipients. Do not conceal mistakes or delete evidence.
2. Contain and safeguard. Recover paper records, revoke inappropriate links, secure accounts and devices, seek deletion from an unintended recipient and involve approved IT support. Protect anyone at immediate risk and alert the DSL. Preserve evidence and record actions.
3. Assess promptly. The Lead considers the nature and volume of information, identifiability, children's vulnerabilities, likely harm, security protections and the effectiveness of containment. Record the risk assessment and revisit it as facts emerge.
4. Notify the ICO unless the breach is unlikely to result in a risk to people's rights and freedoms. Notification must be without undue delay and, where feasible, within 72 hours of awareness, including weekends and holidays. Do not wait for a complete investigation; provide information in phases where necessary and explain delays. Include the nature of the breach, contact point, likely consequences and measures taken.
5. Where likely high risk exists, notify affected individuals without undue delay in clear language with practical protective steps, unless a lawful Article 34 exception applies. Assess safe communication with children and families; record any exception and supporting reasons. Notify commissioners and other controllers or partners where legally or contractually required. A processor acting for us must notify us without undue delay.
6. Log every breach, including non-reportable incidents. Record facts, effects, remedial action, the notification decision, supporting reasons and dates. Assign improvements, check completion and update risk assessments and training. The Lead reports significant incidents to Directors.

Appendix C Appropriate Policy Document requirements

This appendix establishes mandatory controls for processing that requires an Appropriate Policy Document. The Lead must maintain an accompanying processing register identifying each actual Article 6 basis, Article 9 or 10 route, precise Schedule 1 condition, purpose, information category, recipients and retention rule before reliance on that condition. This policy does not assert that every Schedule 1 condition is being used.

Processing must be fair and explained through the relevant notices, subject to lawful safeguarding restrictions. Limit collection and access to the documented purpose; distinguish factual and reported information; check accuracy and correct errors. Apply section 9 security controls and section 8 disclosure controls. The Directors oversee lawful processing and the Lead keeps evidence of decisions and reviews.

Retain information under the relevant Appendix A category and any documented legal hold, with regular review of necessity. Record secure erasure or destruction at expiry, including arrangements with processors. Any departure from the schedule must state why it is needed and when it will be reviewed.

The completed Appropriate Policy Document and associated condition records must be reviewed regularly, kept for the processing period and at least six months afterwards where Schedule 1 requires this, and made available to the ICO on request. Employment health processing and substantial public interest processing must be checked separately for their particular statutory requirements.

Appendix D Reference sources and publication checks

Legal and guidance review completed 4 October 2026. Use the current versions of these official sources when applying the policy.

UK GDPR and Data Protection Act 2018 as amended: www.legislation.gov.uk/eur/2016/679/contents and www.legislation.gov.uk/ukpga/2018/12/contents.

Data (Use and Access) Act 2025: www.legislation.gov.uk/ukpga/2025/18/contents. ICO guidance on its changes and complaints: ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/.

DfE safeguarding sources: www.gov.uk/government/publications/keeping-children-safe-in-education--2; www.gov.uk/government/publications/working-together-to-safeguard-children--2; www.gov.uk/government/publications/information-sharing-to-safeguard-children-and-young-people.

ICO organisational guidance: ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/. DfE retention guidance used as a reference with adaptations: www.gov.uk/guidance/data-protection-in-schools/record-keeping-and-management. DBS certificate handling: www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information.