

Replenish Learning



Information Governance and Data Protection Policy

Policy Version:	2.0
Date of Issue:	September 2025
Review Date:	September 2026
Approved by:	AK (Director)

Replenish Learning

Information Governance and Data Protection Policy

1. Introduction

Replenish Learning is committed to safeguarding the privacy and security of all personal information. This policy outlines how we collect, manage, store, and protect personal data in compliance with UK data protection laws, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other relevant legislation.

2. Purpose

The purpose of this policy is to ensure that Replenish Learning meets its legal, ethical, and professional responsibilities when handling personal data. It explains how we protect information, uphold individuals' rights, and manage data in line with statutory requirements.

3. Scope

This policy applies to all employees, volunteers, contractors, and third-party providers who process personal data on behalf of Replenish Learning. It covers all personal data relating to pupils, parents and carers, staff, governors, visitors, and partners.

4. Legal Framework

Replenish Learning complies with the following laws and regulations:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005
- Protection of Freedoms Act 2012 (for biometric data)
- The Children Act 1989 (for safeguarding)

5. Data Protection Principles

Replenish Learning follows the principles of the UK GDPR, which require that personal data must be:

- Processed lawfully, fairly, and transparently.
- Collected for specified, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Retained only for as long as necessary.
- Processed securely to protect against unauthorised access, loss, or damage.

6. Data Collection and Use

Replenish Learning collects and uses personal data for the following purposes:

- Managing pupil admissions, attendance, progress, and safeguarding.
- Communicating with parents and carers about their child's education and wellbeing.
- Meeting legal and statutory obligations, including safeguarding, SEND provision, and statutory reporting.
- Ensuring the safety and security of pupils, staff, and visitors.
- Managing staff employment records and contractor information.

7. Lawful Basis for Processing

Personal data is processed on the following lawful grounds:

- Consent: Where explicit consent has been obtained for a specific purpose.
- Contractual necessity: To fulfil contractual obligations (e.g., employment or service agreements).
- Legal obligation: To meet statutory duties, such as safeguarding and reporting requirements.
- Legitimate interests: Where processing is necessary for Replenish Learning's operations, provided individual rights are not overridden.

8. Special Category Personal Data

Replenish Learning recognises that some personal data is classed as special category data under the UK GDPR and Data Protection Act 2018. This includes information about health, SEND, ethnicity, religion, and safeguarding records. Such information is processed with additional protection and safeguards.

Where necessary for the safety or welfare of children, we may process and share special category data without consent. The Data Protection Act 2018 (Schedule 1, Part 2) provides 'safeguarding of children and individuals at risk' as a condition for processing special category personal data in these circumstances.

9. Data Security

Replenish Learning ensures that personal data is protected through robust security measures, including:

- Encryption: Protecting sensitive data in transit and at rest.
- Access control: Limiting access to authorised staff only.
- Physical security: Secure storage of paper and electronic records.
- Breach management: A clear procedure for responding to data breaches, including notification to the Information Commissioner's Office (ICO) within 72 hours where required.

10. Information Governance and Retention

To ensure accountability, Replenish Learning implements:

- Data audits: Regular checks on the accuracy and relevance of data.
- Staff training: Ongoing training in data protection, confidentiality, and safeguarding.
- Data retention:
 - Safeguarding records are retained securely until the child's date of birth + 25 years, in line with statutory guidance.
 - Other pupil records created by Replenish Learning are retained for six years after the placement ends.
 - Staff and contractor records are retained for six years after employment or engagement ends.
 - Financial records (including payroll and invoices) are retained for six years in line with HMRC requirements.
 - Record of transfer: Replenish Learning retains a record of transfer for accountability purposes.

11. Privacy and Confidentiality

Replenish Learning is committed to protecting privacy by:

- Sharing information only with those who have a legal right, contractual obligation, or explicit consent to receive it.
- Providing clear privacy notices, including accessible and child-friendly versions, to explain how data is used and individuals' rights.
- Respecting confidentiality by ensuring that information is handled ethically, proportionately, and securely.

In line with Keeping Children Safe in Education 2025:

- Staff understand that timely information sharing is essential to safeguarding.
- Staff are reminded that fear about sharing information must never prevent them from protecting a child's welfare.
- Where appropriate, safeguarding information will be shared with local authorities, CMARS partners, and other agencies.
- Pupils are reassured that concerns will be taken seriously, but staff will never promise confidentiality where sharing information is required to keep them safe.

12. Rights of Data Subjects

Under the UK GDPR, individuals have the right to:

- Be informed about how their data is processed.
- Access their personal data through a Subject Access Request (SAR).
- Request corrections to inaccurate or incomplete information.
- Request erasure ('right to be forgotten') in certain circumstances.
- Request restrictions on processing.
- Object to processing in certain circumstances.
- Request data portability.
- Be protected against decisions made solely by automated processing.

13. Data Sharing and Third Parties

Replenish Learning shares data with third parties for educational, safeguarding, and compliance purposes.

- Third parties must meet our data protection and security requirements.
- Data Processing Agreements are in place where required.
- Where data is transferred outside the UK, Replenish Learning ensures appropriate safeguards are in place.

14. Biometric Data

Where biometric data (e.g. fingerprints for access systems) is used, Replenish Learning complies with the Protection of Freedoms Act 2012 by:

- Seeking explicit written parental consent before collection.
- Using biometric data only for the stated purpose.
- Deleting biometric data securely when no longer required.

15. Monitoring and Review

This policy will be reviewed annually, or sooner if legislation changes, to ensure continued compliance with UK data protection laws and safeguarding requirements.

16. Contact Information

For any questions, concerns, or requests relating to this policy, please contact:

Data Protection Lead (DPL): Atique Kahn Email: a.kahn@replenishlearning.co.uk

Website: www.replenishlearning.co.uk

Appendix A: Data Retention Schedule

Record Type - Retention Period

Safeguarding records - DOB + 25 years

Pupil records - 6 years after placement ends

Staff and contractor records - 6 years after employment ends

Financial records - 6 years (HMRC requirement)

Accident/incident reports - DOB + 25 years

Complaints records - 6 years after resolution

Recruitment records - 6 months after decision

Appendix B - Data Breach Management Procedure

1. Purpose

Replenish Learning is committed to protecting personal data of pupils, parents/carers, staff, and partners. This procedure sets out how we respond to personal data breaches in line with UK GDPR and the Data Protection Act 2018.

2. Definition of a Data Breach

A data breach is a breach of security leading to destruction, loss, alteration, unauthorised disclosure, or access to personal data. Examples include:

- Loss or theft of devices
- Sending personal data to the wrong recipient
- Unauthorised access by a third party
- Loss of paper records
- Accidental alteration or deletion of records

3. Principles

- All breaches must be taken seriously and reported immediately.
- The welfare and safety of children overrides embarrassment or reputational damage.
- Replenish Learning will act in accordance with UK GDPR and safeguarding guidance.
- Where there is risk to individuals' rights, the ICO will be notified within 72 hours.
- Individuals affected will be informed promptly if there is high risk.

4. Roles and Responsibilities

Data Protection Officer (DPO): Atique Kahn, Business Manager.

Designated Safeguarding Lead (DSL): Works with DPO if breaches involve children's records.

All Staff: Must immediately report any suspected breach to the DPO or DSL.

5. Breach Management Procedure

Step 1: Identification and Reporting

- Staff report breaches immediately to the DPO with full details.

Step 2: Containment and Recovery

- The DPO acts to contain the breach and involve IT support where needed.

Step 3: Risk Assessment

- The DPO and DSL assess the severity, considering data type, individuals affected, consequences, and safeguarding implications.

Step 4: Notification

- The DPO notifies the ICO within 72 hours if required.
- Affected individuals are informed if high risk.

Step 5: Documentation

- All breaches are logged in the Data Breach Register.

Step 6: Evaluation and Prevention

- The DPO reviews security measures and provides training as needed.

6. Training and Awareness

All staff receive training on recognising and reporting data breaches during induction and refresher sessions.

7. Policy Review

This procedure will be reviewed annually or sooner if required.

Next Review Date: September 2026