Data Retention Policy

v1.1 · Reviewed Jun 2026 · Next review May 2027

Halved Data Retention Policy

This policy was published in June 2026

1. Purpose

This policy sets out the categories of personal data processed by Halved Limited ("**Halved**") in respect of the Halved platform, and the retention periods that apply to each category or type of personal data, and the procedures by which data is deleted and/or anonymised at the end of each retention period. It supports Halved's compliance with UK data protection legislation and helps demonstrate how we meet our legal and regulatory obligations.

2. Scope

This policy applies to all personal data collected, stored, or processed by Halved in respect of the Halved platform in connection with the delivery of AI-assisted learning support to UK schools. It covers data held in all storage systems operated on behalf of Halved, including by such of our sub-processors Azure PostgreSQL, MongoDB Atlas, Azure Blob Storage, and Azure Cache for Redis. For more details about the use by any of the aforementioned sub-processor, please see our Privacy Policy.

This Policy does not cover Halved's retention of its own internal controller records such as human resources and benefits records, legal and accounting records, and sales and marketing records, which are maintained as internal confidential documents.

3. Data Controller and Processor

Where Halved provides the platform to a school, the school is controller for student personal data and school staff platform data processed in the school tenant, and Halved acts as processor under the school DPA. Halved acts as controller only for its own business administration, website enquiries, sales/contract records, support records, security/compliance records, complaints records and legal/accounting records.

4. Retention Schedule

The table below sets out the retention period for each category of personal data.

Data Category	Data Types	Storage Location	Retention Period	Basis for Retention
Student account data	Name, year group, school, hashed password, account creation date	MongoDB Atlas (Azure UK South)	Duration of school contract + 90 days (unless the school instructs earlier deletion or return)	School documented instructions as set out within the data processing agreement in accordance with UK GDPR Art. 28
Chat messages and session transcripts	Student messages, AI responses, session identifiers, timestamps	MongoDB Atlas (Azure UK South)	Duration of school contract + 90 days (unless the school instructs earlier deletion or return)	School documented instructions as set out within the data processing agreement in accordance with UK GDPR Art. 28; or safeguarding audit retention only where enabled and instructed by school
Student profile analysis	Learning style summary, subject observations derived from session data	Azure PostgreSQL (UK)	Duration of school contract + 90 days (unless the school instructs earlier deletion or return)	School documented instructions as set out within the data processing agreement in accordance with UK GDPR Art. 28
Lesson materials	Uploaded curriculum content	Azure PostgreSQL + Azure Blob	Duration of school contract + 90	School documented instructions as

Data Category	Data Types	Storage Location	Retention Period	Basis for Retention
	linked to student sessions	Storage (UK South)	days (unless the school instructs earlier deletion or return)	set out within the data processing agreement in accordance with UK GDPR Art. 28
Safeguarding flags	Flagged message excerpts, category, severity, session reference, timestamp, status	Azure PostgreSQL (UK)	As instructed by the school and aligned with the school safeguarding retention policy (if applicable)	School documented instructions as set out within the data processing agreement in accordance with UK GDPR Art. 28; or (as applicable) For compliance with a legal obligation; safeguarding regulatory guidance (Keeping Children Safe in Education)
Authentication tokens	Session tokens, JWT identifiers stored in Redis	Azure Cache for Redis (UK South)	Session JWT expires after 7 days	Strictly necessary for security and session management
Application logs	App Service diagnostic logs (no PII in log body, see Logging Policy)	Azure Log Analytics Workspace (UK South)	30 days (unless a security incident requires longer retention of	Security and operational monitoring; data minimisation

Data Category	Data Types	Storage Location	Retention Period	Basis for Retention
			relevant extract)	
Email delivery records	Delivery status, message ID, recipient address for transactional emails sent via Azure Communication Services	Azure Communication Services (United Kingdom)	30 days	Transactional delivery, support and security audit
Teacher and staff accounts	Name, email address, role, school, hashed password	MongoDB Atlas (Azure UK South)	Duration of school contract + 90 days (unless the school instructs earlier deletion or return)	School documented instructions as set out within the data processing agreement in accordance with UK GDPR Art. 28
School administrator accounts	Name, email address, administrator role, school identifier	MongoDB Atlas (Azure UK South)	Duration of school contract + 90 days (unless the school instructs earlier deletion or return)	School documented instructions as set out within the data processing agreement in accordance with UK GDPR Art. 28;
Security incident records	Incident ID, severity, affected systems/accounts, timeline, containment and remediation actions, notification assessment,	Restricted security incident log / compliance storage	7 years from incident closure unless a shorter or longer period is required by law,	Security incident management, UK GDPR accountability, regulatory evidence and legal claims

Data Category	Data Types	Storage Location	Retention Period	Basis for Retention
	resolution and lessons learned. Avoid student chat content, SEND/accessibility data, passwords, tokens or secrets except where strictly necessary.		regulator, insurer, school DPA or legal proceedings	
Administrative access records and access reviews	Admin Account Register, access grants/removals, role, system, start and end dates, monthly contractor access reviews, MFA/access control evidence and privileged-access audit information	Access management records / approved register	3 years from access removal, or up to 6 years where needed for audit, legal claims, regulatory investigation or Cyber Essentials evidence	Security, Cyber Essentials, audit and UK GDPR accountability

5. Post-Contract Deletion

Upon termination or expiry of the school's contract with Halved, all personal data subject to the "Duration of school contract + 90 days" retention period will be permanently deleted within 90 calendar days of the contract end date. The 90-day window allows for:

Resolution of any outstanding data subject access requests or complaints;

Transition assistance to the school or its successor provider;

Final invoicing and contractual close-out.

Deletion will be performed by permanently removing the relevant records from MongoDB Atlas, Azure PostgreSQL, and Azure Blob Storage.

6. Safeguarding Data

Safeguarding flags are retained in accordance with the relevant UK school instructions provided to Halved as set out within the data processing agreement ('**DPA**') agreed between Halved and the school, or otherwise in accordance with the relevant UK school's documented lawful instructions. The specific retention periods for safeguarding flags are as set out within the relevant DPA or are otherwise aligned to the relevant school's safeguarding retention policy and/or documented instructions. In the event of any conflict between the retention periods set out within the DPA between Halved and the relevant school, the DPA shall prevail, unless and to the extent that Halved and the school agree otherwise.

Access to safeguarding records after contract termination will be restricted to the designated safeguarding leads of the contracting school and to Halved's designated safeguarding officer.

7. Deletion Verification

Halved will maintain a deletion log recording the date, scope, and method of each deletion event. The deletion log itself does not contain personal data and records only the school identifier, the data categories deleted, and the timestamp. The log will be retained for 3 years.

Where a school or data subject requests confirmation of deletion, Halved will provide written confirmation within 30 days following the date of deletion.

8. Sub-processor Retention and Deletion

All sub-processors used by Halved are bound by the Microsoft Customer Agreement and Microsoft Data Protection Addendum, which include obligations to delete personal data in accordance with the controller's documented instructions. MongoDB Atlas is bound by MongoDB's Data Processing Agreement.

Halved will issue written deletion instructions to relevant sub-processors within 30 days of a contract end date. Sub-processors are required to confirm deletion within their own documented SLAs.

9. Backup Retention

Automated backups are retained as follows:

**MongoDB Atlas: **Point-in-time restore enabled with a 7-day restore window. Backups are stored within Azure UK South.

**Azure PostgreSQL: **Automated backups are retained for 7 days with geo-redundant storage within the UK.

**Azure Blob Storage: **No automatic backup; data durability provided by Azure LRS (locally redundant storage) within UK South.

No backup snapshot will be retained beyond the applicable retention period for the data category it contains.

10. Data Subject Rights and Early Deletion

For further information about the rights of data subjects, please see our Privacy Policy.

In respect of any requests received by Halved from a data subject to exercise their right to erasure (including when such request is received from a student, a parent and/or legal guardian) Halved will comply with all such requests and delete the specific personal data without undue delay and in any event within one month of receipt of the request. This period may be extended by up to two further months where the request is complex or numerous, in which case Halved will inform the data subject within one month of receipt and explain the reasons.

Requests for the erasure of any special category personal data retained by Halved or any of its sub-processors will be complied with without delay (and in any event, within one month of receipt of any request).

There may be circumstances where Halved has a legal obligation to retain information (excluding special category information) which will result in Halved having to refuse to comply with an erasure request. In such circumstances, Halved will inform the data subject without delay and shall set out the reasons for such refusal. The circumstances that may be relied upon for such refusal include (but are not limited to) compliance with applicable laws and/or regulations, or for establishing, exercising or defending legal claims.

11. Policy Review

This policy is reviewed annually (or upon a material change to the Halved platform’s data processing activities, applicable law, or regulatory guidance). The next scheduled annual review is May 2027.

12. Document Control

| Field | Detail |

| Document title | Halved Data Retention Policy | | Version | 1.1 | | Date | June 2026 | | Author | Halved Limited | | Owner | Halved Limited | | Classification | Confidential, for DPO review | | Next review | May 2027 |

Questions about data protection? **dataprivacy@halved.io**

Website **halved.io** · students log in at my.halved.io

Halved Limited · registered in England and Wales, company number 15261677 · last updated June 2026