halved

INFORMATION GOVERNANCE

Information Governance Pack

One place for the documentation your data protection and information security review needs. Read online, download individual files, or download the complete pack as a single file.

halved

Cookie Policy

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

Cookie Policy

Version 1.1 | June 2026

Our website can be found at: https://www.halved.io.

Halved uses only strictly necessary cookies. These are needed for the platform to work, for example to keep you securely signed in and to protect the service against malicious traffic. Halved does not use analytics, advertising or tracking cookies, does not use cookies to build a profile of you, and does not track your activity across other websites.

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer's hard drive.

We use the following cookies:

- Strictly necessary cookies.

You can find more information about the individual cookies we use and the purposes for which we use them in the table below:

Cookie	Purpose	Type	Duration
__Host-next-auth.csrf-token	Protects the sign-in process against cross-site request forgery.	Strictly necessary	Session
__Secure-next-auth.callback-url	Supports secure sign-in redirection.	Strictly necessary	Session
__Secure-next-auth.session-token	Keeps you securely signed in to the platform.	Strictly necessary	Up to 7 days
cf_clearance	Set by Cloudflare to keep the service secure and protect it against malicious traffic.	Strictly necessary (set by Cloudflare)	Up to 1 year

Please note that third parties (such as embedded content providers) may also use cookies, over which we have no control. These third-party cookies are likely to be strictly necessary or functionality cookies.

Review

This Cookie Policy is reviewed at least once a year, and sooner if the cookies we use or the applicable law change. The next scheduled review is June 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

Data Flow and Data Handling Summary

v3.0 · Reviewed Jun 2026 · Next review Jun 2027

For school IT leads and Data Protection / Designated Safeguarding Leads

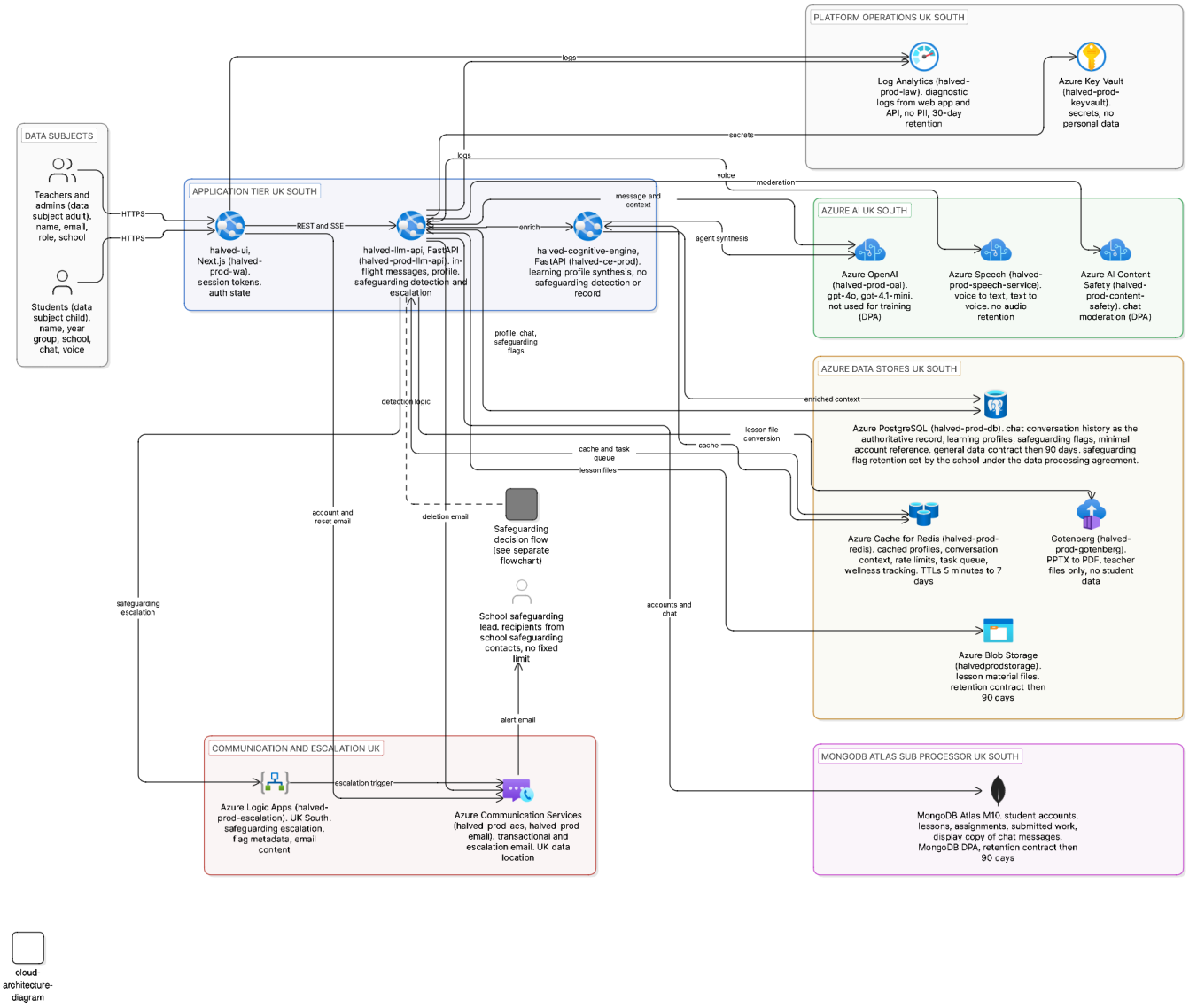
Version 3.0 | June 2026

Overview

Halved is an always available learning support system that brings expert guidance to every student at the exact moment they need it. This document describes what data Halved collects, where it is stored, how it is processed, and how it is protected. It is intended to support your school's data protection assessment and due diligence process.

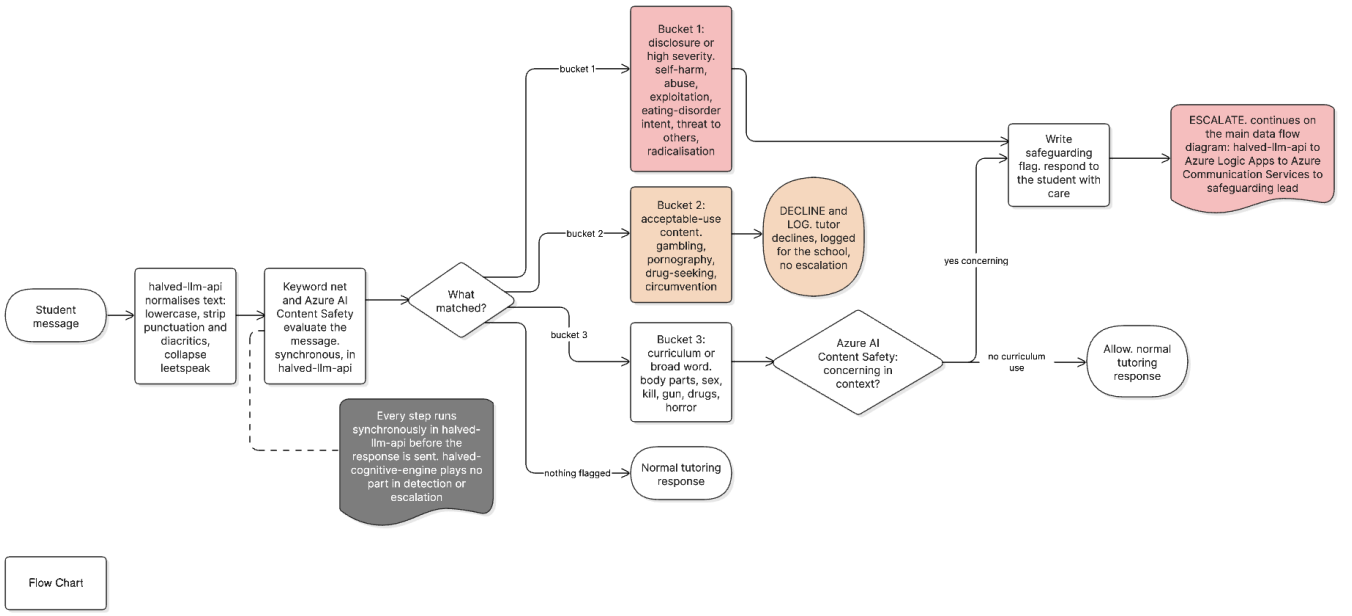
All data storage and all data processing, including artificial intelligence inference and voice processing, takes place within the United Kingdom. No student personal data is stored or processed outside the United Kingdom.

Data Flow Diagram



The Halved platform architecture and data flow, showing how data moves between the student's browser, the Halved application layer, and Microsoft Azure UK South services.

Safeguarding Decision Flowchart



How student messages are checked in real time: detection via Azure AI Content Safety, severity assessment, and escalation to the school's Designated Safeguarding Lead.

1. What data Halved holds about students

When a student account is created, Halved stores:

- Name and email address, used for login only.
- Year group and subject assignments, set by the teacher.
- Assignment work, the written work the student produces within Halved.
- Chat conversation history, the text of conversations between the student and Halved's learning support.
- A learning profile, a background summary built by Halved from how the student interacts during tutoring. It records observed learning behaviour only, such as topics covered, apparent strengths, areas of difficulty, preferred ways of learning, and recent engagement. It does not record any medical diagnosis, neurodevelopmental condition, or disability label. This summary is used to personalise future sessions and is held within Microsoft Azure UK South.

Halved does not collect:

- Biometric data.
- Location data.
- Device identifiers beyond a standard browser session.
- Payment information.

2. Where data is stored

All data is stored within the Microsoft Azure UK South region (London datacentres), or on MongoDB Atlas hosted in Azure UK South. No student personal data is stored outside the United Kingdom.

What	Storage technology	Location
Student accounts, lessons, assignments, submitted work, and the display copy of conversation messages shown in the interface	MongoDB Atlas	Azure UK South
Full chat conversation history as the authoritative turn-by-turn record, learning profiles derived from conversations, and safeguarding flags	Azure Database for PostgreSQL	Azure UK South
Uploaded lesson files (PPTX, PDF)	Azure Blob Storage	Azure UK South
Temporary cache, conversation context, rate limiting, and background task queue	Azure Cache for Redis	Azure UK South
Secrets and credentials	Azure Key Vault	Azure UK South
Application and audit logs	Azure Log Analytics Workspace	Azure UK South

All data is encrypted at rest. Secrets such as API keys, passwords, and encryption keys are stored in Azure Key Vault and never stored in plain text.

3. AI and voice processing

All AI inference and voice processing is performed within Microsoft Azure UK South. No student data is transmitted to servers outside the United Kingdom for AI or voice processing.

AI chat processing, Azure OpenAI (UK South)

When a student sends a message to Halved's learning support, that message, along with structured context about the lesson topic, assignment criteria, and the student's learning profile, is transmitted to the Microsoft Azure OpenAI Service, hosted in Azure UK South (London datacentres).

What is sent to Azure OpenAI:

- The student's message text, exactly as typed.
- Lesson notes and assignment criteria for the current task.
- A summary of the student's learning profile, expressed as observed learning behaviour (for example, that the student benefits from shorter explanations).
- A role-based identifier, a unique ID, not the student's name.

What is not sent to Azure OpenAI:

- The student's name or email address as structured fields.
- Diagnoses or condition labels. Halved is configured so that diagnosis and condition labels are never written into the learning profile or transmitted to the AI service.
- Submitted work from previous assignments.
- Any data not directly relevant to the current tutoring session.

Azure OpenAI Service is governed by the Microsoft Data Processing Addendum. Data sent via the Azure OpenAI API is not used by Microsoft to train foundation models, and Halved does not use student data to train third-party models.

Halved operates as a closed-loop tutoring system: it does not browse the internet and does not return public-search results.

Note: if a student types their name or personal details directly into the chat box, that text will be included in what is sent to Azure OpenAI, because Halved processes the message as written. Students should be advised not to include personal information in chat messages.

Voice features, Azure Speech Service (UK South)

Halved supports optional voice features, both processed entirely within Azure UK South:

- Speech to text, a student speaking their answer, processed via the Microsoft Azure Speech Service, UK South region.
- Text to speech, Halved reading content aloud, using the Microsoft Azure Speech Service (voice: en-GB-AdaMultilingualNeural), UK South region.

Voice features are optional. If your school prefers to disable them, this can be requested.

4. How access is controlled

Students and teachers log in with an email address and password.

- Passwords are stored using bcrypt hashing and are never stored or transmitted in plain text.
- Sessions use encrypted JSON Web Tokens with a seven-day expiry.
- Communication between Halved's web app and AI backend uses an internal API key, not exposed to the browser.
- Teacher accounts and student accounts are role-separated. Teachers can view only their own students' work.
- System administrator access is separately controlled and limited to Halved staff.

5. Safeguarding

Halved includes a live safeguarding pipeline operating across all environments. Student messages are checked in real time. Where a welfare concern is detected, the concern is logged and an alert is sent to the school's nominated safeguarding lead or leads. Lower-severity concerns are flagged and escalated without interrupting the student's session. Higher-severity concerns return appropriate support information to the student and are escalated immediately.

The safeguarding pipeline uses Azure AI Content Safety and Azure Logic Apps, both hosted in Azure UK South and covered by the Microsoft Data Processing Addendum. Safeguarding alert content, including a short excerpt of the flagged message, is sent to the school's nominated safeguarding contacts by email through Azure Communication Services (United Kingdom).

6. Data security summary

| Control | Status |

| Encryption at rest | Yes, all Azure storage | | Encryption in transit | Yes, HTTPS/TLS throughout | | Secrets management | Azure Key Vault | | Password storage | bcrypt hashed | | Role-based access control | Yes, student, teacher, admin | | UK data residency (all storage and processing) | Yes, Azure UK South and MongoDB Atlas Azure UK South |

7. Data retention and deletion

Halved retains student personal data for the duration of the school's contract. Following termination of services, general personal data is securely deleted within 90 days, unless Halved is required to retain it for longer to comply with legal, accounting, or regulatory requirements.

Safeguarding records are treated differently. Where a safeguarding concern has been recorded, the associated record is retained in line with statutory safeguarding guidance (Keeping Children Safe in Education) and the school's own retention schedule, which is typically up to seven years. This applies regardless of the general deletion timeline above.

Requests for deletion of an individual student's data during the contract period (the right to erasure under UK GDPR) should be directed to dataprivacy@halved.io. Halved will action these requests without undue delay and in any event within one month of receipt, extendable by up to two further months for complex or numerous requests. Where a record is subject to a statutory safeguarding obligation, Halved may retain it to the extent required by law. The school, as controller, determines the retention and erasure of safeguarding records, as set out in the Data Processing Agreement and aligned to the school's safeguarding retention schedule and Keeping Children Safe in Education.

In some circumstances, Halved may anonymise personal data so that it can no longer be associated with any individual. Anonymised data may be retained indefinitely and used to improve the platform.

8. Third-party services and sub-processors

All third-party services used by Halved process data within the United Kingdom and are covered by a Data Processing Agreement. A full sub-processor register is available on request.

Service	Purpose	Location	Student data involved	DPA
Microsoft Azure (App Service, PostgreSQL, Redis, Blob, Key Vault, Log Analytics)	Application hosting, primary data storage, secrets management	UK South	All student and teacher data	Microsoft DPA
Azure OpenAI Service	AI learning support responses	UK South	Chat messages, lesson context, learning profile summary	Microsoft DPA
Azure Speech Service	Speech to text and text to speech	UK South	Student voice audio, AI-generated text	Microsoft DPA
Azure AI Content Safety	Safeguarding and content moderation of messages	UK South	Chat message content	Microsoft DPA
Azure Logic Apps	Safeguarding escalation workflow to the school's Designated Safeguarding Lead	UK South	Safeguarding alert content and flagged message excerpts	Microsoft DPA
Azure Communication Services	Transactional emails (account creation, password reset) and safeguarding escalation emails to school leads	United Kingdom	User email addresses, names, account setup links, safeguarding alert content	Microsoft DPA
Azure Container Instances (Gotenberg)	Lesson material document conversion, PPTX and PDF converted to page images for display	UK South	Teacher-uploaded lesson material content	Microsoft DPA

Service	Purpose	Location	Student data involved	DPA
MongoDB Atlas	Student accounts, lessons, assignments, submitted work, and the display copy of conversation messages	Azure UK South	All structured student and teacher data	MongoDB DPA
Cloud202 (technical contractor)	Production infrastructure management, deployment, and Terraform state	London UK	Administrative access to production systems holding student and teacher data	Data Processing Agreement

9. Contact

For data protection questions related to your pilot, or to request a Data Processing Agreement, please contact:

Halved Limited

dataprivacy@halved.io

Registered in England and Wales, company number 15261677.

10. Review

This summary is reviewed at least once a year, and sooner when the platform architecture, data processing activities or sub-processors change. The next scheduled review is June 2027.

This document reflects the technical architecture of the Halved platform as at June 2026.

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

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

Data Protection Complaints Process

v1.0 · Reviewed Jun 2026 · Next review Jun 2027

Halved Limited

Data Protection Complaints Process

Version 1.0 | June 2026 |
Owner: Andrew James, CEO. Contact: dataprivacy@halved.io

1. Purpose and scope

This document sets out how Halved Limited (Companies House no. 15261677) handles data protection complaints. It has been produced to meet the requirements of section 103 of the Data (Use and Access) Act 2025 (which inserts section 164A into the Data Protection Act 2018), which comes into force on 19 June 2026, and supports compliance with UK GDPR Article 5(2) (accountability). It supplements the complaints section of the Halved Privacy Policy.

This process applies to complaints from any individual whose personal data Halved processes, including students, parents, teachers, school staff, and website visitors. Where Halved acts as data processor for a school, certain complaints will be co-ordinated with the school as controller, as described below.

2. How to make a complaint

If you are unhappy about how Halved has handled your personal data, please contact us using any of the following routes:

- Email: dataprivacy@halved.io
- Post: Data Protection, Halved Limited, 4 Comet House, Calleva Park, Aldermaston, Berkshire, RG7 8JA

Please include your name and contact details, a description of your concern, and any relevant dates or reference numbers. You do not need to use any specific form or format.

If you are a student, parent or legal guardian with a question about student data held within the school platform, please contact your school first. Your school is the data controller for student platform data. Halved will assist the school in responding to the complaint.

3. What happens after we receive your complaint

Halved will handle your complaint in the following stages:

- **Acknowledgement.** We will acknowledge receipt of your complaint within 30 days of receiving it. Our acknowledgement will confirm that we have received your complaint and will give you a reference number or contact name.
- **Investigation.** We will investigate your complaint without undue delay. We may contact you to ask for additional information if needed to investigate properly. We will keep you informed of progress.
- **Response.** We will tell you the outcome of our investigation without undue delay. Our response will explain what we found, what action (if any) we have taken or intend to take, and how to escalate to the ICO if you remain unsatisfied.

We will aim to resolve complaints as quickly as possible. If your complaint is complex or requires input from a third party such as your school, we will let you know and keep you updated on timing.

4. School-related complaints (controller co-ordination)

Where Halved acts as a data processor for a school, the school is the data controller for students and school staff platform data. If your complaint concerns data that the school has directed Halved to process, Halved will:

- acknowledge your complaint in line with the timescales in section 3;
- notify the relevant school promptly so that the school, as controller, can assist in responding;
- co-ordinate its response with the school; and
- provide you with a response and, where relevant, direct you to the school's own data protection complaints process or to the school's Data Protection Officer.

You can also contact your school directly. Most schools will have a data protection contact or Data Protection Officer who can assist with complaints about student data. Their contact details should be available from the school.

5. If you are not satisfied with our response

If you are not satisfied with the outcome of your complaint, or if we have not responded within the timeframe above, you have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection.

- Website: https://www.ico.org.uk/make-a-complaint/
- Telephone: 0303 123 1113
- Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

We would always prefer to have the opportunity to address your concern first. Raising your complaint with us directly before escalating to the ICO will usually result in a faster resolution.

6. Complaint records

Halved keeps a record of all data protection complaints received, including the date of receipt, the nature of the complaint, the steps taken to investigate and resolve it, and the outcome. This log is reviewed as part of Halved's data protection governance and compliance activities. Complaint records are retained for a minimum of three years from the date of resolution.

7. Making this process available

This process is published on the Halved website and is referenced in the Halved Privacy Policy. It is written in plain language and is available in alternative formats on request.

Contact dataprivacy@halved.io to request a large-print, audio or other accessible version.

8. Review

This process will be reviewed annually or when data protection requirements change.

Next review: June 2027.

Halved Limited is registered in England and Wales (Companies House no. 15261677). Registered office: 4 Comet House, Calleva Park, Aldermaston, Berkshire, RG7 8JA.

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

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

Privacy Policy

v1.2 · Reviewed Jun 2026 · Next review Jun 2027

Version 1.2 | June 2026

Halved Limited ("**Halved**") is the operator of the Halved platform and website. Where Halved processes personal data as controller, it is the organisation legally responsible for deciding how and why that personal data is used. Where Halved processes student and school staff platform data for a school, the school is controller and Halved is processor, as explained below.

We are **Halved Limited** (hereafter referred to as "**Halved**", "**we**", "**us**", "**our**") and we are committed to protecting personal data. This privacy notice explains how personal data is collected, used, shared, stored and protected when schools, teachers, school administrators, students and website visitors use the Halved platform at https://www.halved.io, contact us, or use our website.

This notice applies to school administrators, teachers, students and website visitors. It should be read alongside the relevant school privacy notice. For students, parents and legal guardians, the school remains the first point of contact for questions about how student data is used in the school setting.

What this notice covers

This notice applies to personal data processed through the Halved platform and website. It does not replace the school's privacy notice. It also does not apply to third-party websites or services linked from Halved; those organisations are responsible for their own privacy information.

This version is mainly written for adults, including school staff, parents and legal guardians. Halved will also make student-facing privacy information available before or when students first use the platform, in a concise, age-appropriate form for students using the platform.

Who are we?

Controller and processor status. For personal data processed through a school tenant for the purpose of delivering AI-assisted learning support to that school, the school is the controller and Halved acts as processor under a written data processing agreement. This includes student account data, teacher-created assignments, student assignment work, chat history and AI learning profiles. Halved processes that data only on the school documented instructions, except where UK law requires otherwise. Halved is controller for personal data it processes for its own business purposes, including website enquiries, news updates, supplier and customer administration, sales records, security administration and compliance records.

If you have any questions about this privacy notice or our privacy practices, please contact us:

Legal entity: **Halved Limited**

Email: dataprivacy@halved.io

Registered office address: 4 Comet House, Calleva Park, Aldermaston, Berkshire, RG7 8JA.

If you are a student, parent or legal guardian and your question concerns student data held in the school platform, please contact the school first. Halved will assist the school in responding to validated requests.

How do we use your data?

Personal data we collect and how it is collected

The personal data processed by Halved depends on how you interact with the platform and website. It may include names, school email addresses, school, year group, role, account details, hashed passwords, teacher-created assignment allocations, assignment work and submitted content, chat messages and AI responses, AI-generated learning profile summaries, optional voice audio where voice features are enabled, safeguarding alert content and metadata, support and enquiry details, news-update preferences, technical and security logs, and cookie or usage information.

Personal data is collected directly from schools and teachers when they configure tenants, classes, assignments and accounts; directly from students when they use the platform; directly from you when you contact Halved or sign up to updates; and automatically from the website or platform through necessary logs, session technologies and cookies.

Where personal data is needed to provide the platform, administer an account, respond to an enquiry, keep the service secure or comply with law, failure to provide it may mean that the relevant service or functionality cannot be provided. Where personal data is optional, Halved will make this clear and explain any effect of declining to provide it.

School and teacher accounts: For platform access, we process names, school email addresses, role, school identifier, hashed password and account administration information. Where this relates to the school use of the platform, Halved acts as processor for the school. Where Halved uses school contact details for contract administration, service notices, support, billing, security management or legal compliance, Halved acts as controller and relies on contract necessity, legitimate interests and/or legal obligation, as applicable.

Student accounts: Student accounts are created or authorised by the school. We process student name, school email address, year group, school and subject/assignment allocations. The platform does not capture SEND, accessibility, health or disability flags, and the AI learning profile records observed learning behaviour only and does not record any diagnosis, neurodevelopmental condition or disability label. The school is responsible for identifying the relevant Article 6 lawful basis; Halved processes student data only on the school documented instructions and applies appropriate confidentiality, access control, minimisation and security safeguards.

Platform usage and AI learning support: When students and teachers use the platform, Halved processes assignment work, chat conversation history, AI responses, lesson context, role-based identifiers, session timestamps and AI-generated learning profile summaries. The AI learning profile is inferred from the student's use of the platform and is used to personalise future learning support sessions, such as by giving shorter explanations or identifying topics that may need reinforcement. Halved does not use identifiable student personal data to train third-party foundation models or for independent product development. Any service-improvement analysis using student-derived data must be carried out only on an anonymised or aggregated basis, unless the school has given documented instructions for the specific processing.

News updates: If you sign up to receive our news updates, we collect your name and email address to send them to you. We rely on consent or another lawful basis permitted by PECR and UK GDPR. You can unsubscribe at any time by using the unsubscribe link in our emails or by emailing dataprivacy@halved.io.

Contact enquiries and support: When you contact us by email, through our website or through a support channel, we collect your name, contact details and the content of your enquiry so that we can respond, administer our services and keep appropriate records. We rely on legitimate interests, contract necessity and/or legal obligation depending on the nature of the enquiry.

Website cookies

For more information about our deployment of and use of cookie information, please see Cookie Policy.

Controller purposes and lawful bases - more detail

The following table gives further detail about Halved controller processing. Student and school staff platform data processed for a school remains subject to the school DPA and the school documented instructions.

What Halved uses personal data for	Relevant personal data	Role and lawful basis
Providing and administering school-facing platform access for school staff	Staff names, school email addresses, role, school identifier, account and support information	Processor for school platform data. As controller for customer administration: contract necessity, legitimate interests and legal obligation, as applicable.
Responding to enquiries and support requests	Contact details, role, school or organisation, enquiry content and support records	Legitimate interests, contract necessity and/or legal obligation, depending on the nature of the request.
News updates and adult marketing communications	Name, email address, organisation, role and communication preferences	Consent or legitimate interests where permitted by UK GDPR and PECR. Students must not receive marketing through the platform.
Non-essential cookies, website analytics and similar technologies	Cookie identifiers, browser/device information and website usage information	Consent where required by PECR and UK GDPR. Strictly necessary cookies are used to provide the service.
Security, audit logging, fraud prevention and incident response	Account identifiers, session information, audit logs, security events and technical metadata	Legal obligation and legitimate interests in keeping the platform secure and protecting users, schools and Halved.
Legal claims, regulatory compliance, accounting, audit and corporate administration	Relevant account, contact, transaction, correspondence and compliance records	Legal obligation and legitimate interests in protecting, managing and evidencing Halved's business and legal rights.
Student-facing platform data processed for a school	Student account data, assignments, chat history and AI learning profiles	Halved acts as processor under the school's documented instructions. The school identifies the Article 6 lawful basis.

When Halved relies on legitimate interests as controller, it will assess whether its interests are overridden by the rights and interests of the relevant individual. You may request information about that assessment by contacting Halved.

Special category data

The platform is not designed to capture special category data and does not collect SEND, accessibility, health or disability flags. The AI-generated learning profile records observed learning behaviour only and does not record any diagnosis, neurodevelopmental condition or disability label. Halved does not solicit special category data. Where a student includes sensitive information in a free-text message, that content is handled through the safeguarding pipeline and Halved's security controls; in that limited context the school, as controller, is responsible for identifying any applicable Article 9 condition and DPA 2018 Schedule 1 condition, and Halved processes such content only on the school documented instructions.

No sale or advertising use

Halved will not sell student personal data, use student personal data for behavioural advertising, or use student personal data to train third-party foundation models.

Approved applications and AI tools

Halved's internal approved applications list does not authorise staff or contractors to process student personal data, school-controlled personal data or confidential school materials in general-purpose AI tools, social media tools, Dropbox or other non-platform applications. Those tools must not be used with student data unless separately assessed, approved, covered by appropriate contractual terms and, where required, added to the school DPA and sub-processor register.

Marketing and news updates

Halved will not send marketing or news updates to students through the platform. Adult school contacts and website visitors may receive news updates or service information where permitted by UK GDPR and PECR.

You can opt out of marketing communications at any time by using the unsubscribe link in Halved emails or by contacting dataprivacy@halved.io. This will not affect non-marketing service messages, security notices or communications that Halved is required or permitted to send for contractual, operational or legal reasons.

Halved will not sell personal data or share personal data with third parties for their own marketing purposes.

Processing children's data

The Halved platform is used by students, including children under the age of 18. Student accounts are created and managed by schools and teachers, not directly by students or parents. Halved processes student personal data only for school educational purposes and on the school's documented instructions. The following section gives further detail about use of generative AI in an education setting, including child-appropriate safeguards.

Personal data processed in an education setting

This section explains how personal data is processed where Halved is deployed by a school to provide AI-assisted learning support. It is intended to supplement, not replace, the school's own privacy notice. The school remains the controller for student and school staff platform data and determines the educational purposes and lawful basis for the processing. Halved acts as processor for that school-controlled data under a written data processing agreement, except where Halved separately acts as controller for its own administration, security, legal compliance or business records.

Data subjects who may be affected

The processing may involve students who use the platform, including children aged under 18 and students with SEND or accessibility needs; teachers, tutors, school administrators and designated safeguarding leads who configure or supervise use of the platform; parents or legal guardians where their details or correspondence are provided by the school or included in a support or safeguarding context; and Halved personnel or authorised technical support users whose access is recorded in audit and security logs.

Types of personal data processed

Depending on the school configuration and features enabled, Halved may process identity and account data, such as name, school email address, role, school, year group, class and account credentials; educational data, such as teacher-created assignments, lesson context, assignment criteria, submitted work, quiz or task responses and teacher feedback; chat content, including student prompts, AI responses and conversation history; inferred learning data, including AI-generated learning profile summaries about apparent strengths, areas of difficulty and preferred learning approaches; optional voice audio and AI-generated audio where speech features are enabled; safeguarding alert content, message excerpts and escalation metadata; and technical data such as session times, role-based identifiers, security events, audit logs and diagnostic metadata.

How the generative AI works

Halved is a closed-loop educational support tool. It does not browse the internet, does not return public search results and does not use identifiable student personal data to train third-party foundation models. When a student sends a message to the AI, Halved sends the message text, relevant lesson notes, assignment criteria, the immediate conversation context, a role-based student identifier and a limited summary of the student's learning profile to Azure OpenAI Service in the UK South region. Halved does not send the student's name or email address as structured fields to Azure OpenAI. However, if a student types personal information into a chat message, that information will form part of the message text processed by the AI service.

Explanation of the AI output

The AI generates natural-language responses by predicting helpful text from the instructions, lesson materials and conversation context supplied to it. The output is not a human decision, is not guaranteed to be error-free, and should not be treated as an official educational assessment, disciplinary decision or safeguarding determination. The AI-generated learning profile is an inferred summary used to adapt future learning support, for example by providing shorter explanations, checking understanding, or revisiting topics that appear difficult. It is not intended to diagnose, label or determine a student's SEND, disability or health status, and it is not used to make decisions with legal or similarly significant effects about students. Teachers and schools remain responsible for supervising the learning activity, reviewing outputs where appropriate and making educational, pastoral and safeguarding decisions.

Third-party sub-processors used to provide the platform and generative AI

Halved uses the sub-processors listed in the section “Who do we share personal data with?”. For generative AI and related platform delivery, these include Microsoft Azure for hosting, storage, security, logging and infrastructure; MongoDB Atlas for structured platform data; Azure OpenAI Service for AI learning support responses; Azure Speech Service where optional speech-to-text or text-to-speech is enabled; Azure Communication Services for transactional and safeguarding escalation emails; Azure Container Instances/Gotenberg for document conversion of teacher-uploaded lesson materials; Azure AI Content Safety and Azure Logic Apps for the safeguarding pipeline; Cloud202 Ltd for authorised technical development, support and maintenance. Cloudflare provides DNS, CDN and security for the Halved website (halved.io) only and does not process student or school personal data through the platform. Planned or conditional providers must not process live student data until assessed, contractually covered and activated in accordance with the school DPA and sub-processor notification arrangements.

Lawful basis

Where Halved processes student and school staff platform data for a school, Halved acts as processor and relies on the school’s documented instructions rather than identifying its own Article 6 lawful basis for that school-controlled processing. The school is responsible for identifying and communicating its lawful basis. In many UK state school deployments, the relevant lawful basis is likely to be public task under Article 6(1)(e) UK GDPR, although schools must make their own assessment. Independent schools or other education providers may in some cases rely on legitimate interests, contract necessity, legal obligation or another lawful basis depending on the circumstances.

The platform does not capture SEND, accessibility, health or disability flags. Where safeguarding information or other sensitive information is processed, for example where a student includes such information in a free-text message, the school is responsible for identifying an Article 9 condition and any required Data Protection Act 2018 Schedule 1 condition, such as substantial public interest conditions relevant to safeguarding.

Where Halved acts as controller for its own business, security, support, legal or compliance purposes, the lawful bases are set out in the controller purposes and lawful bases section above.

Children's Code (Age-Appropriate Design Code) safeguards

Halved will apply the following child-privacy safeguards where the platform is used by children, including where those safeguards are adopted as good practice to support the school's own compliance with the ICO Children's Code (Age-Appropriate Design Code). In particular, Halved will place students' best interests at the centre of design and operation; support the school with DPIA information and data flow documentation; provide concise, prominent and age-appropriate privacy information, including point-of-use explanations for AI personalisation/profiling and prompts to ask a teacher or trusted adult if a student is unsure; use high-privacy defaults; collect and use only the personal data needed for the educational purpose; avoid using student data for advertising, sale of data, behavioural profiling, unrelated analytics or independent model training; restrict profiling to explainable learning-support personalisation; avoid nudge techniques that encourage students to weaken privacy settings or share unnecessary personal data; not collect geolocation, biometric data, payment data or device identifiers beyond what is needed for a standard browser session; limit sharing to approved sub-processors; apply role-based access controls, encryption, audit logging and retention limits; and provide routes for students, parents and schools to raise concerns or exercise data protection rights through the school.

School configuration and supervision

Schools should decide which classes, subjects, students and features are appropriate for the deployment, including whether optional voice features are enabled. The safeguarding pipeline is a standard, always-active part of the platform, and each school must provide at least one designated safeguarding lead and a monitored email address to receive safeguarding alerts. Schools should tell students not to include unnecessary personal information in chat messages and should ensure teachers understand that AI outputs are support materials requiring professional oversight, not a substitute for teacher judgement or safeguarding procedures.

Who do we share personal data with?

We share personal data with the following categories of third parties:

- **Technology providers and sub-processors**: We use the technology providers listed below to operate, host, support and secure the platform. Where student data is processed for a school, these providers act as sub-processors and must be covered by written data processing terms. Planned or conditional providers must not process live student data

until they are activated under the school DPA (and the school has been notified where required).

Provider	Purpose	Location	Data involved
Microsoft Azure	Primary hosting, storage, security services, audit logging and infrastructure services	UK South / United Kingdom regions, as configured	Platform data required to host, secure and operate the service
MongoDB Atlas	Student accounts, lessons, assignments and structured platform data	Azure UK South	Structured platform data as configured for the school tenant
Azure OpenAI Service	AI learning support responses and language model inference	UK South	Chat messages, lesson context, role-based identifier and learning profile summary. Student names and email addresses are not sent as structured fields.
Azure Speech Service	Optional speech-to-text and text-to-speech voice features	UK South	Student voice audio and AI-generated text where the school enables voice features
Azure Communication Services	Transactional emails and safeguarding escalation emails	United Kingdom	Usernames, email addresses, account setup/password reset links and safeguarding alert content
Azure Container Instances (Gotenberg)	Document conversion for teacher-uploaded lesson materials	UK South	Teacher-uploaded lesson material content
Azure AI Content Safety	Automated content safety moderation	UK South	Chat message text and safety metadata
Azure Logic Apps	Safeguarding workflow orchestration if enabled	UK South	Safeguarding flag metadata and escalation email content

Provider	Purpose	Location	Data involved
Cloud202 Ltd ** (‘Cloud202**’)	Technical platform development, support and infrastructure maintenance where access to personal data is required	United Kingdom	Potential access to platform data for support and maintenance under Halved instructions and Article 28/sub-processor terms. No independent use, download, reuse or retention of student data; access must be named, MFA-protected, least privilege and reviewed.
Cloudflare (website only)	DNS, CDN and security for the Halved marketing website (halved.io)	Active for the website; not in front of the platform	IP addresses, headers and security metadata of website visitors. Does not process student or school personal data.

Cloud202 access to personal data is permitted only under appropriate Article 28/sub-processor terms, documented access controls, MFA, least privilege and removal of temporary contractor access when no longer required.

Cloudflare fronts the Halved marketing website (halved.io) only and does not sit in front of the student-facing platform (my.halved.io). It therefore processes no student or school personal data and is not a platform sub-processor. This was confirmed in June 2026 by inspecting response headers, which showed Cloudflare serving halved.io but not my.halved.io.

Regulators and authorities: We may share personal data where required by law or where necessary for safeguarding, security, prevention or detection of crime, legal claims, or to protect rights, property or safety. Where Halved is processor, such disclosures will be made in accordance with the DPA, documented instructions or applicable law, and we will inform the school unless legally prohibited.

Halved only allows service providers and sub-processors to handle personal data where Halved is satisfied that they take appropriate measures to protect it and where appropriate contractual obligations are in place. Where Halved acts as processor, sub-processors must be authorised under the school DPA or notified to the school in accordance with that DPA.

Halved may also share relevant personal data with professional advisers, insurers, auditors, banks, law enforcement agencies, courts, public authorities and regulators where necessary for legal, regulatory, accounting, audit, insurance, safeguarding, security or dispute-resolution purposes.

If Halved undergoes a merger, acquisition, asset sale, investment, restructuring or insolvency process, relevant personal data may be shared with the other parties and professional advisers involved. Halved will limit the information shared where possible and will require appropriate confidentiality protections.

Where do we store your data?

Data residency and international transfers: Production data is hosted in UK regions as described in the Data Flow and Data Handling Summary. Halved will not intentionally host student personal data outside the UK. If any restricted transfer arises, including support access from outside the UK, Halved will ensure appropriate safeguards under Chapter V UK GDPR are in place and will notify the school where required by the DPA.

International transfers - more detail

The current position is that production student personal data is hosted in UK regions. If Halved needs to transfer personal data outside the UK in the future, including support access from outside the UK, Halved will do so only where an adequacy regulation, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another lawful transfer mechanism applies.

Halved will not permit access to UK school or student personal data by any non-UK affiliate or operation unless the school has been notified where required and appropriate UK GDPR transfer safeguards and processor or sub-processor arrangements are in place.

How long do we keep your data?

Retention: Student and school staff platform data is retained in accordance with the school contract, the school documented instructions and the Halved Data Retention Policy. Unless a longer period is required by law or the school documented instructions, school-controlled personal data will be deleted or returned within 90 days after termination of the school contract. Safeguarding records must be retained only for the period agreed with the school and aligned with the school safeguarding retention schedule.

Anonymisation: Halved may retain information indefinitely only where it has been anonymised so that individuals are no longer identifiable, taking account of the risk of singling out, linkability, and inference. Pseudonymised data remains personal data and is not treated as anonymised. Halved must not attempt to reidentify anonymised information.

AI profiling and automated decision-making: Halved creates an AI-generated learning profile from a student's interactions with the platform to personalise learning support. This is profiling/inferred data for data protection purposes, as explained in the section "Personal data processed in an education setting". It is not used to make decisions with legal or similarly significant effects about a student and does not replace teacher judgement. Teachers and schools remain responsible for educational decisions.

Keeping personal data secure

Halved uses appropriate technical and organisational measures designed to prevent personal data from being accidentally lost, used, accessed, altered or disclosed unlawfully. These include encryption in transit, encryption at rest, role-based access controls, secrets management, audit logging and controlled administrator access, as described in Halved's Security Policy.

Access to personal data is limited to people and providers with a genuine need to access it for the purposes described in this notice and, where relevant, under the school DPA. Halved also maintains procedures to deal with suspected personal data breaches.

Administrative and contractor access to production systems is restricted to authorised personnel with a need to know and must use named accounts, MFA, least privilege, password-manager storage, access logging/review and timely removal of temporary contractor access.

Where Halved acts as processor for a school, Halved will notify the school without undue delay after becoming aware of a personal data breach affecting school-controlled personal data. Where Halved acts as controller, Halved will notify affected individuals and/or the ICO where legally required.

What are your rights under data protection law?

Where Halved acts as controller, you may have the rights listed below. Where Halved acts as processor for a school, requests about student or school staff platform data should be made to the school, and Halved will assist the school in responding.

- **Request access to your personal data (subject access request)**: to receive a copy of the data we hold and to check we are processing it lawfully.
- **Request correction**: to have incomplete or inaccurate data corrected.
- **Request erasure**: to ask us to delete your personal data where there is no good reason to continue processing it. Note that we may not always be able to comply for specific legal reasons, which we will explain if applicable.
- **Object to processing**: where we rely on legitimate interest, or where we process your data for direct marketing.
- **Request restriction of processing**: to ask us to suspend processing in certain circumstances.
- **Request data portability**: to receive your data in a structured, machine-readable format where applicable.
- **Withdraw consent**: where we rely on consent. This will not affect the lawfulness of any processing before withdrawal.

You also have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects, where applicable. Halved does not use the platform to make such decisions about students.

You also have the right to lodge a complaint. For more information, please see the section 'How to complain' below.

Please be aware that these rights are not absolute and will not be available in all circumstances.

To exercise a right where Halved is controller, please email dataprivacy@halved.io and provide enough information to identify yourself, the right you want to exercise and the personal data to which your request relates. Halved may request additional information if reasonably needed to verify your identity.

Halved will respond to valid rights requests without undue delay and normally within one month, subject to any extension permitted by UK GDPR for complex requests. Where Halved is processor for a school, Halved will assist the school in responding to validated requests.

How to complain

You have the right to make a complaint to us if you are unhappy about how we handle your personal data. You can contact us at dataprivacy@halved.io. We will acknowledge your complaint within 30 days of receiving it and, without undue delay, will take appropriate steps to investigate, keep you informed and tell you the outcome. Full details of how we handle data protection complaints are set out in our Data Protection Complaints Process, available on our website.

You also have the right to complain to the Information Commissioner's Office, the UK supervisory authority for data protection. The ICO can be contacted through https://www.ico.org.uk or by telephone on 0303 123 1113.

Do we review this policy?

We review this privacy notice at least once a year, and sooner when our practices change or when required by law. The next scheduled review is June 2027. We will notify schools of material changes affecting school-controlled personal data in accordance with the school DPA. When Halved makes significant changes, it will take appropriate steps to inform schools and, where relevant, website users, for example by notifying school contacts or publishing a notice on the Halved website.

Do you need extra help?

If you would like this notice in another format, such as large print, audio, accessible HTML or another language, please contact dataprivacy@halved.io.

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

Sub-processor Register

v1.3 · Reviewed Jun 2026 · Next review May 2027

Version 1.3 | June 2026 | Owner: Andrew James, CEO

This register lists all third-party organisations (sub-processors) that process personal data on behalf of Halved Limited in connection with the Halved platform. It is maintained in accordance with Article 28 of UK GDPR and is reviewed annually or when sub-processors change.

Halved will provide schools with notice of any new or replacement sub-processor in accordance with the data processing agreement ('**DPA**') agreed between Halved and the school and allow any objection rights set out in that DPA before the sub-processor processes live student data.

Any planned or conditional sub-processor must not process live student data until the relevant DPA terms are in place and the school has been notified where required.

Conditional providers must be marked active only if the relevant service is enabled in a way that processes platform personal data.

Sub-processor Register

Sub-processor	Parent entity	Services used	Purpose	Data categories processed	Location	DPA	Status
Microsoft Azure	Microsoft Corporation	App Service, PostgreSQL Flexible Server, Cache for Redis, Blob Storage, Key Vault, Log Analytics Workspace	Application hosting, primary data storage, secrets management, audit logging	Student names, email addresses, accessibility flags, assignment work, chat history, AI learning profiles, session data, API credentials	UK South (London)	Microsoft DPA	Active
Azure OpenAI Service	Microsoft Corporation	Azure OpenAI (gpt-4o, gpt-4.1-mini)	AI learning support inference, generating responses to student messages	Chat message text, lesson context, learning profile summary, role-based student identifier	UK South (London)	Microsoft DPA	Active
Azure Speech Service	Microsoft Corporation	Speech-to-text, Text-to-speech (en-GB-AdaMultilingualNeural)	Converting student voice input to text; converting AI text responses to audio	Student voice audio recordings, AI-generated text content	UK South (London)	Microsoft DPA	Active
Azure Communication Services	Microsoft Corporation	Email send (ACS)	Transactional emails (account creation, password reset, sign-in reminders); safeguarding escalation emails to school leads	User email addresses, names, account setup links, password reset tokens; safeguarding alert content and flagged message excerpts	United Kingdom	Microsoft DPA	Active
Azure Container Instances (Gotenberg)	Microsoft Corporation	Azure Container Instances running Gotenberg:8 document converter	Converting teacher-uploaded lesson materials (PPTX, PDF) into page images for in-platform display	Lesson material content (teacher-uploaded educational files)	UK South (London)	Microsoft DPA	Active
Azure AI Content Safety	Microsoft Corporation	Content Safety API	Automated moderation of student chat messages	Chat message text	UK South (London)	Microsoft DPA	Active

Sub-processor	Parent entity	Services used	Purpose	Data categories processed	Location	DPA	Status
			and AI responses for safeguarding categories				
Azure Logic Apps	Microsoft Corporation	Logic Apps workflow	Orchestrating safeguarding escalation flow triggered by high-severity flags	Safeguarding flag metadata, email content	UK South (London)	Microsoft DPA	Active
MongoDB Atlas	MongoDB, Inc.	Atlas M10 cluster (halved-prod-mongodb)	Primary document store for student accounts, lessons, assignments, and chat history	Student names, email addresses, accessibility flags, assignment work, chat conversation history, AI learning profiles	Azure UK South (London)	MongoDB DPA	Active
Cloud202 Ltd	Cloud202 Ltd	Infrastructure management, deployment, and Terraform state	Production infrastructure management and technical support	Administrative access to production systems holding student and teacher data	London, UK	Data processing agreement	Active (temporary)

DPA References

Microsoft Products and Services Data Protection Addendum: microsoft.com/licensing/docs (covers all Azure services listed above under a single Microsoft DPA)

MongoDB Data Processing Agreement: mongodb.com/legal/data-processing-agreement

Notes

Azure AI Content Safety and Azure Logic Apps support the live safeguarding pipeline and are active sub-processors.

No sub-processors are located outside the United Kingdom.

This register covers the production environment (halved-prod-rg, Azure UK South). Development and demo environments process no real student data.

Halved does not use any sub-processor for analytics. Google Analytics and Microsoft Clarity have been removed from the platform.

Cloudflare provides DNS, CDN and security for the Halved marketing website (halved.io) only. It does not sit in front of the student-facing platform (my.halved.io) and processes no student or school personal data, so it is not a platform sub-processor. Confirmed June 2026 by response-header inspection (cf-ray present on halved.io, absent on my.halved.io).

**Review date: **May 2027 (or earlier if sub-processors change) | dataprivacy@halved.io

halved

Admin Account Usage Policy

v1.0 · Reviewed Jun 2026 · Next review Jun 2027

HALVED LIMITED

ADMINISTRATIVE ACCOUNT USAGE POLICY

Version: 1.0 Effective Date: 4th June 2026 Last Review: 4th June 2026 Next Review: 4th June 2027

Owner: Andrew James, CEO

1. PURPOSE

This policy defines how administrative accounts must be used at Halved Limited to maintain security and comply with Cyber Essentials requirements.

2. SCOPE

This policy applies to all users with administrative access to Halved systems, including:

- macOS devices
- Microsoft 365 / Azure
- GitHub
- MongoDB Atlas
- Cloudflare
- Other cloud services requiring administrative access

3. POLICY REQUIREMENTS

3.1 Separate Admin Accounts

Every user requiring administrative access MUST have two separate accounts:

- Standard Account: For daily work (email, messaging, browsing, coding, collaboration)
- Admin Account: ONLY for administrative tasks (installing software, changing system configurations, creating/deleting accounts, modifying security settings)

3.2 Admin Account Naming Convention

- macOS: andrew-admin (local account)
- Cloud services: andrew-admin@halved.io

3.3 Prohibited Activities on Admin Accounts

Admin accounts must NOT be used for:

- Sending or receiving email
- Web browsing
- Messaging (Slack, Teams, WhatsApp, etc.)
- Writing code or documents
- Any daily work activities

3.4 Permitted Activities on Admin Accounts

Admin accounts may ONLY be used for:

- Installing or uninstalling software
- Changing system configurations
- Creating or deleting user accounts
- Modifying security settings
- Performing system updates
- Other explicitly administrative tasks

3.5 Admin Account Session Management

- Log into admin account only when performing an admin task
- Log out immediately after the task is complete
- Do not leave admin accounts logged in

- Maximum admin session duration: 30 minutes

3.6 Admin Account Security

- All admin accounts MUST have multi-factor authentication (MFA) enabled
- Admin account passwords must be at least 12 characters
- Admin account passwords must be unique (not shared with any other account)
- Admin account passwords must be stored in a password manager

3.7 Temporary Contractor Access

- Temporary contractors (e.g., Cloud202 team) with admin-level access for specific project work:
- Are documented in the Admin Account Register with start and end dates
- Have their access reviewed monthly during the contract period
- Have all access removed within 24 hours of contract end
- Are subject to this policy during their engagement

4. COMPLIANCE

Violation of this policy may result in:

- Immediate revocation of admin access
- Disciplinary action
- Cyber Essentials certification failure

5. REVIEW SCHEDULE

This policy will be reviewed annually and updated as needed.

APPROVED BY:

Andrew James, CEO Halved Limited Date: 6th May 2026

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

halved

Approved Applications List

v1.1 · Reviewed Jun 2026 · Next review Aug 2026

Document owner: Andrew James, CEO

Version: 1.1 Last updated: 4th June 2026 Review frequency: Quarterly (next review: August 2026)

APPROVED APPLICATIONS - MACOS (MacBook Air 15" M4)

Productivity & Communication:

- Microsoft Outlook (Microsoft 365 subscription)
- Microsoft Word (Microsoft 365 subscription)
- Microsoft Excel (Microsoft 365 subscription)
- Microsoft PowerPoint (Microsoft 365 subscription)
- Microsoft Teams (Microsoft 365 subscription)
- Slack (team communication)
- Zoom (video conferencing)

Browsers:

- Safari (built-in with macOS)
- Google Chrome (Version 148.0.7778.168 or later)

Development & Technical:

- Visual Studio Code (code editing)
- GitHub Desktop (version control)
- MongoDB Compass (database management)

Cloud & File Management:

- Microsoft OneDrive (Microsoft 365 subscription)
- Dropbox (if used)

Business Tools:

- Figma (design)
- Miro (collaboration)
- Loom (video recording)
- DocuSign (document signing)

AI & Productivity:

- Claude Desktop
- Perplexity
- ChatGPT (OpenAI)

Utilities:

- Apple Passwords (built-in password manager)
- NordVPN (network security)

Approval method: All applications from App Store or identified developers with valid code signatures. Gatekeeper enforces technical control.

APPROVED APPLICATIONS - iOS/iPadOS (iPhone 16 Pro Max, iPad A16)

Productivity & Communication:

- Microsoft Outlook (App Store)
- Microsoft Word (App Store)
- Microsoft Excel (App Store)
- Microsoft PowerPoint (App Store)
- Microsoft Teams (App Store)

- Slack (App Store)
- Zoom (App Store)

Browser:

- Safari (built-in with iOS/iPadOS)

Cloud & File Management:

- Microsoft OneDrive (App Store)
- Dropbox (App Store - if used)

Business Tools:

- Figma (App Store)
- Miro (App Store)
- Loom (App Store)
- DocuSign (App Store)

Social Media (Business Use):

- LinkedIn (App Store)
- X/Twitter (App Store)
- Instagram (App Store)
- Threads (App Store)
- YouTube (App Store)
- Reddit (App Store)
- TikTok (App Store)
- Pinterest (App Store)
- Medium (App Store)
- Bluesky (App Store)

AI & Productivity:

- ChatGPT (App Store - if installed)
- Claude (App Store - if installed)
- Perplexity (App Store - if installed)
- Plaud (App Store - if installed)

Security:

- Microsoft Authenticator (App Store - MFA)
- Google Authenticator (App Store)
- NordVPN (App Store)

Approval method: All applications must be installed from Apple App Store only. iOS/iPadOS enforces technical control - no sideloading permitted.

TECHNICAL CONTROLS ENFORCING APPLICATION APPROVAL

MacBook Air:

- macOS Gatekeeper enabled and set to “App Store and identified developers”
- System Integrity Protection (SIP) active
- Unsigned applications blocked by default
- Administrator approval required for any exceptions

iPhone & iPad:

- iOS/iPadOS App Store is ONLY installation method
- Sideloading disabled (no developer mode)
- All apps code-signed by Apple
- Users cannot install apps from other sources

APPROVAL PROCESS FOR NEW APPLICATIONS

- User identifies need for new application
- CEO reviews application: security, business need, vendor reputation
- CEO verifies application is code-signed (Mac) or from App Store (iOS/iPadOS)
- CEO approves installation
- Application added to this approved list
- User installs application

REMOVAL PROCESS

- Applications are removed if:
- No longer needed for business purposes
- Vendor ends support or security updates
- Security vulnerability identified
- User no longer requires access

Quarterly reviews identify applications for removal.

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

halved

Logging Policy

v1.0 · Reviewed Jun 2026 · Next review Jun 2027

HALVED LIMITED

LOGGING POLICY

Version: 1.0 Effective Date: 9th June 2026 Last Review: 9th June 2026 Next Review: 9th June 2027

Owner: Andrew James, CEO

1. PURPOSE

This policy defines how Halved Limited (“Halved”) generates, stores, protects and retains log data for the Halved platform. It supports Halved’s compliance with the security and integrity principle under Article 5(1)(f) and Article 32 UK GDPR, the school data processing agreement, and Cyber Essentials-aligned controls. It is referenced by, and read alongside, the Halved Data Retention Policy and the Halved Security Policy.

2. SCOPE

This policy applies to all logs generated by the production components of the Halved platform hosted in Microsoft Azure UK South, and to the development and demo environments to the extent they generate logs. It covers application and diagnostic logs, security and audit logs, deployment activity logs, email delivery records and security incident records.

3. LOGGING PRINCIPLES

- **Data minimisation.** Logs capture only what is needed to operate, secure and support the platform.

- **No student personal data in log bodies.** Application and diagnostic logs must not contain student names, email addresses, chat or message content, assignment work, learning profiles, accessibility or SEND flags, or any special category data. Role-based and system identifiers may appear where needed for diagnosis.
- **No secrets in logs.** Passwords, API keys, tokens and encryption keys are never written to logs.
- **UK data residency.** All platform logs are stored within the United Kingdom.
- **Integrity and confidentiality.** Logs are encrypted in transit and at rest, and access is restricted and reviewed.

4. PASSWORD CREATION GUIDANCE

4.1 Creating Strong Passwords

Log type	Contents	Store	Retention
Application and diagnostic logs	App Service runtime and diagnostic events. No personal data in the log body.	Azure Log Analytics Workspace (UK South)	30 days, unless a security incident requires longer retention of a relevant extract
Security and audit logs	Authentication and authorisation events, administrative actions and other security-relevant events. No student content.	Azure Log Analytics Workspace / Azure Monitor (UK South)	30 days. Security incident extracts retained per the Security Incident Response Policy
Deployment activity	CI/CD pipeline runs, deployments and approvals	GitHub Actions audit logs	Per GitHub retention
Email delivery records	Delivery status, message ID and recipient address for transactional and safeguarding escalation emails	Azure Communication Services (United Kingdom)	30 days
Security incident records	Incident ID, severity, affected systems, timeline, actions and resolution. Avoids student content, accessibility/SEND data, passwords, tokens or secrets except where strictly necessary.	Restricted security incident log / compliance storage	7 years from incident closure

Safeguarding flags and flagged message excerpts are held in the safeguarding records described in the Data Flow and Data Handling Summary and the Data Retention Policy, not in general application logs.

5. WHAT IS NOT LOGGED

- Student chat or message content in application or diagnostic logs.

- Student names or email addresses as structured fields in diagnostic logs.
- Accessibility or SEND flags, learning profiles, or other special category data.
- Passwords, API keys, tokens or encryption keys.

6. ACCESS TO LOGS

Access to logs is restricted to authorised Halved personnel and authorised technical contractors with a genuine need, using named accounts, multi-factor authentication and least privilege, in line with the Administrative Account Usage Policy. Access is itself logged and reviewed. Where Halved acts as processor for a school, log access for support and maintenance is under the school's documented instructions and the data processing agreement.

7. MONITORING AND REVIEW

Application and security logs are monitored for anomalies and operational issues. Access logs and security configurations are reviewed regularly to identify unauthorised activity. Availability and health alerts route to the CEO.

8. RETENTION AND DELETION

Log retention periods are set out in section 4 and in the Data Retention Policy, which prevails in the event of any conflict. Logs are deleted automatically at the end of their retention period. Security incident records are retained and disposed of in line with the Security Incident Response Policy.

9. REVIEW

This policy is reviewed annually, or on a material change to the platform, applicable law or regulatory guidance. Next review: June 2027.

APPROVED BY:

Andrew James, CEO Halved Limited Date: 9th June 2026

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

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

halved

Password Policy

v1.0 · Reviewed Jun 2026 · Next review Jun 2027

HALVED LIMITED

PASSWORD POLICY

Version: 1.0 Effective Date: 4th June 2026 Last Review: 4th June 2026 Next Review: 4th June 2027

Owner: Andrew James, CEO

1. PURPOSE

This policy defines password requirements for all Halved Limited systems to protect against unauthorised access and meet Cyber Essentials requirements.

2. SCOPE

This policy applies to all passwords used to access:

- Halved email accounts (Microsoft 365)
- Cloud services (Azure, GitHub, MongoDB Atlas, Cloudflare, Xero, etc.)
- macOS user accounts
- Any other systems containing organisational data

3. PASSWORD REQUIREMENTS

3.1 Minimum Password Standards

All passwords must meet the following minimum requirements:

- Minimum length: 10 characters
- No maximum length restriction

- Complexity: Use a passphrase (three or more random words) OR a mix of upper/lowercase letters, numbers, and symbols
- Uniqueness: Each system must have a unique password - never reuse passwords across services

3.2 Multi-Factor Authentication (MFA)

- MFA is required on all systems that offer it
- **Preferred MFA method:** Authenticator app (Microsoft Authenticator, Google Authenticator, or similar)
- **Acceptable MFA method:** SMS codes (where authenticator app is not available)
- **Not acceptable:** Email-based MFA does not count as true MFA

3.3 Password Management Requirement

All users must:

- Use a password manager to store passwords securely
- **Recommended password managers:** 1Password, Bitwarden, or macOS Keychain
- Never store passwords in plain text (documents, spreadsheets, notes apps)
- Never share passwords via email, Slack, or messaging

3.4 Admin Account Passwords

Administrative accounts require additional security:

Minimum length: 12 characters (must be different from standard account passwords)

MFA: Mandatory on all admin accounts

Uniqueness: Admin account passwords must be completely different from standard account passwords

4. PASSWORD CREATION GUIDANCE

4.1 Creating Strong Passwords

Good approaches:

- **Three random words:** CorrectHorseBatteryStaple
- **Passphrases:** ILove2DrinkCoffeeInTheMorning!
- **Password manager generated:** Let your password manager create a random strong password

Avoid:

- **Common patterns:** Password123, CompanyName2026
- **Personal information:** birthdays, names, addresses
- **Keyboard patterns:** qwerty123, asdfgh
- **Dictionary words on their own:** elephant (too weak without additional characters)

4.2 Password Expiry

- No forced password changes: Passwords do not expire on a schedule
- Change immediately if: You suspect your password has been compromised
- Change immediately if: A service reports a breach

5. COMPROMISED PASSWORDS

If you suspect your password has been compromised:

- Report immediately: Notify the CEO (Andrew James) within 1 hour
- Change the password immediately on the affected account
- Check for reuse: If you reused the password elsewhere, change it on all systems
- Re-enrol MFA if MFA may have been compromised
- Monitor account activity for unusual behaviour

6. NEW USER ONBOARDING

When a new team member joins:

- They are provided with this Password Policy during onboarding

- They set up a password manager before accessing any Halved systems
- They enable MFA on all accounts during first login
- CEO verifies MFA is enabled before granting access to sensitive systems

7. COMPLIANCE

Failure to comply with this policy may result in:

- Account suspension
- Disciplinary action
- Cyber Essentials certification failure

8. TRAINING

All users receive password security training:

- During onboarding (new users)
- Annually (refresher for existing users)
- After any security incident

APPROVED BY:

Andrew James, CEO Halved Limited Date: 4th June 2026

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

Security Incident Response Policy

v1.0 · Reviewed Jun 2026 · Next review Jun 2027

HALVED LIMITED

SECURITY INCIDENT RESPONSE POLICY

Version: 1.0 Effective Date: 4th June 2026 Last Review: 4th June 2026 Next Review: 4th June 2027

Owner: Andrew James, CEO

1. PURPOSE

This policy defines how Halved Limited responds to security incidents to minimise impact, recover quickly, and prevent future incidents.

2. SCOPE

This policy applies to all security incidents affecting:

- User accounts (email, cloud services, system access)
- Devices (MacBooks, mobile devices)
- Cloud infrastructure (Azure, MongoDB, GitHub, etc.)
- Organisational data

3. WHAT IS A SECURITY INCIDENT?

A security incident includes:

- Suspected account compromise (unauthorised access)
- Lost or stolen device
- Suspected malware infection

- Phishing attack (clicked link, provided credentials)
- Data breach or unauthorised data access
- Suspicious system behaviour
- Ransomware or attempted ransomware
- Any event that could compromise data confidentiality, integrity, or availability

4. INCIDENT RESPONSE PROCEDURE

Phase 1: IMMEDIATE ACTIONS (Within 15 Minutes)

Step 1: Report the Incident

Who to contact: Andrew James, CEO

How to report:

- Email: aj@halved.io
- Phone: +971 585616250
- WhatsApp: +971 585616250

What to report:

- What happened (brief description)
- When it happened
- Which account/system is affected
- What you've done so far (if anything)

Step 2: Initial Containment

CEO takes immediate action:

If account compromised:

- Force password reset on affected account
- Terminate all active sessions

- Disable account temporarily if necessary

If device lost/stolen:

- Remotely wipe device (if possible via Find My / MDM)
- Disable all accounts accessible from that device
- Change passwords for all accounts

If malware suspected:

- Disconnect device from network immediately
- Do not shut down (preserves evidence)
- Notify CEO for next steps

Phase 2: INVESTIGATION (Within 1 Hour)

Step 3: Assess the Scope

CEO investigates:

- Which accounts were accessed?
- What data was accessed or exposed?
- Was the incident isolated or part of a broader attack?
- Were any changes made to systems or data?

Step 4: Document the Incident

Create incident record documenting:

- Date and time incident discovered
- Date and time incident occurred (if different)
- Affected systems/accounts
- Actions taken
- Timeline of events

Phase 3: REMEDIATION (Within 4 Hours)

Step 5: Remove Threat and Restore Access

For compromised accounts:

- Create new strong password (12+ characters, unique)
- Re-enrol MFA (new device/app)
- Review account settings for unauthorised changes
- Check for forwarding rules (email), API keys, etc.
- Re-enable account for legitimate user

For lost/stolen devices:

- Confirm remote wipe completed
- Issue replacement device
- Restore from backup
- Re-enrol in security systems

For malware:

- Run anti-malware scan
- If infection confirmed, wipe and reinstall OS
- Restore from clean backup
- Re-enrol in security systems

Step 6: Verify System Integrity

- Check for backdoors or persistence mechanisms
- Verify no unauthorised users were created
- Confirm no data was exfiltrated (if possible)
- Review logs for suspicious activity

Phase 4: NOTIFICATION (Within 72 Hours if Required)

Step 7: Determine Notification Requirements

Internal notification:

- Notify all team members if incident affects shared systems
- Brief on what happened and what action they need to take

External notification (if required by law):

- Customer data breach: Notify affected customers within 72 hours (GDPR requirement)
- Regulatory reporting: Notify ICO if required under GDPR
- Partner notification: Notify schools/partners if their data affected

When to notify authorities:

- Ransomware attack: Consider reporting to National Cyber Security Centre (NCSC)
- Financial fraud: Report to Action Fraud
- Critical infrastructure impact: Report to NCSC

Phase 5: POST-INCIDENT REVIEW (Within 1 Week)

Step 8: Lessons Learned

CEO conducts review:

- What was the root cause?
- How was the incident detected?
- What worked well in the response?
- What could be improved?
- What preventive measures should be implemented?

Step 9: Update Policies and Procedures

Based on lessons learned:

- Update this policy if needed

- Update technical controls
- Provide additional training to team
- Document improvements in incident record

Step 10: Close Incident

Mark incident as resolved in incident log when:

- Threat has been eliminated
- Normal operations restored
- Required notifications completed
- Lessons learned documented
- Preventive measures implemented

5. INCIDENT SEVERITY LEVELS

Level 1: CRITICAL

- Customer data breach
- Ransomware attack
- Complete system compromise
- Financial fraud

Response time: Immediate (drop everything)

Level 2: HIGH

- Single account compromise with admin access
- Device lost/stolen
- Suspected malware
- Attempted phishing attack (credentials entered)

Response time: Within 1 hour

Level 3: MEDIUM

- Single standard account compromise
- Failed login attempts
- Suspicious email received (not clicked)
- Minor configuration error

Response time: Within 4 hours

Level 4: LOW

- Spam email
- Suspicious but verified legitimate activity
- General security question

Response time: Next business day

6. ESCALATION CONTACTS

Primary Contact:

Andrew James, CEO

Email: aj@halved.io

Phone: +971 585616250

Regulatory Reporting:

ICO (Data Protection): https://ico.org.uk/make-a-complaint/data-protection-complaints/

NCSC (Cyber Security): https://www.ncsc.gov.uk/section/about-ncsc/report-an-incident

7. INCIDENT LOG

All security incidents are logged in: Halved_Security_Incident_Log.xlsx

Minimum information recorded:

- Incident ID (sequential number)
- Date/time discovered

- Date/time occurred
- Severity level
- Brief description
- Affected systems/accounts
- Actions taken
- Resolution date
- Lessons learned

Retention: Incident logs retained for 7 years (GDPR compliance)

8. TRAINING AND AWARENESS

All team members receive security awareness training:

- On joining: Security incident recognition and reporting procedures
- Annually: Refresher on common threats (phishing, social engineering, etc.)
- After incident: Specific training based on lessons learned

9. POLICY REVIEW

This policy is reviewed:

- Annually: Scheduled review every 12 months
- After major incident: Review within 1 week of any Level 1 or Level 2 incident
- When regulations change: Update to reflect new legal/regulatory requirements

APPROVED BY:

Andrew James, CEO Halved Limited Date: 4th June 2026

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

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

halved

Security Policy

v2.0 · Reviewed Jun 2026 · Next review Jun 2027

Version 2.0 | Last Updated: June 2026 | Owner: Andrew James, CEO

1. Introduction

This Security Policy outlines the strategies and measures implemented by Halved Limited ("**Halved**") to protect personal data and ensure the confidentiality, integrity, availability and resilience of the Halved platform. It supports Halved compliance with Article 32 UK GDPR, the school DPA, Cyber Essentials-aligned controls and relevant data protection legislation. Security controls must be appropriate to the processing of children's personal data, accessibility/SEND-related information, chat history, AI learning profiles and AI safety risks.

Reference to "the platform" within this Security Policy is a reference to the Halved platform deployed by Halved for the provision of the AI learning support services provided to UK schools.

2. Scope

This policy applies to all production components of the Halved platform and to any development, staging, support or demo environment that may access or process personal data, including components of the Halved platform as follows:

Microsoft Azure infrastructure (UK South region)

Halved web application: Next.js frontend (halved-prod-wa, production; halved-dev-wa, development)

Halved AI backend: Python/FastAPI service (halved-prod-llm-api, production; halved-dev-llm-api, development)

MongoDB Atlas: primary document store for student accounts, lessons, and chat history (Azure UK South)

Azure PostgreSQL Flexible Server: chat message history and AI learner profiles

Azure Cache for Redis: session caching and background task broker

Azure Blob Storage: uploaded lesson materials (PPTX, PDF)

Azure Key Vault: secrets and credential management

Azure Speech Service: speech-to-text and text-to-speech (UK South)

Azure OpenAI Service: AI learning support responses (UK South)

Azure Log Analytics Workspace: application and audit log ingestion (UK South)

Azure Communication Services: transactional and operational email delivery (United Kingdom)

Azure Container Instances (Gotenberg): lesson material document conversion, PPTX/PDF to page images (UK South)

Cloudflare - DNS/domain administration and, if enabled for the platform, proxy, CDN, WAF, bot protection and access logging. If Cloudflare processes platform personal data, it must be covered by the Sub-processor Register and appropriate data processing terms.

Cloud202 Ltd - technical development, maintenance and support if access to personal data is required.

3. Security Principles

We adhere to the following core security principles:

**Least Privilege Access: **access rights are granted based on the minimum necessary for users to perform their role.

**Zero Trust Architecture: **all internal and external communications are treated as untrusted until verified, ensuring stringent access controls.

**Defence in Depth: **multiple layers of security controls are applied across infrastructure, application, and data layers.

4. Data Protection Measures

4.1 Data Encryption

**At rest: **all data at rest is stored on Azure Storage and encrypted by default using Azure Storage Encryption. Encryption keys are managed via Azure Key Vault.

**In transit: **TLS 1.2 or higher is used for all HTTP communications between users and the platform, and between internal services.

4.2 Data Storage

The platform uses the following primary data stores, all hosted within Azure UK South:

Store	Technology	Data held
Student accounts, lessons, assignments, messages	MongoDB Atlas (Azure UK South)	All structured student and teacher data
Chat history, AI learner profiles	PostgreSQL (Azure Flexible Server, UK South)	Conversation history, background learner analysis
Session cache, background tasks	Azure Cache for Redis (UK South)	Session data, task queue
Uploaded files	Azure Blob Storage (UK South)	Lesson materials (PPTX, PDF) and processed page images
Secrets and credentials	Azure Key Vault (UK South)	API keys, passwords, encryption keys
Application and audit logs	Azure Log Analytics (UK South)	Application logs, deployment activity

4.3 Password Storage

User passwords are stored using bcrypt hashing. Passwords are never stored or transmitted in plain text.

5. Access Control

5.1 Authentication and Role-Based Access

User authentication is handled via NextAuth.js using email address and password credentials. The platform enforces role-based access control with three roles: student, teacher, and system administrator. Teachers can access only their own students' data. System administrator access is limited to Halved staff. Sessions use encrypted JSON Web Tokens (JWT) with a 7-day expiry. API communication between the web application and AI backend is authenticated using an internal API key that is not exposed to the browser.

5.2 Secure Development Practices

Security checks are embedded in the CI/CD pipeline (GitHub Actions) to ensure security criteria are met before deployment

Code is reviewed before merging to the main branch

Secrets are never stored in version control; all credentials are managed via Azure Key Vault

Resource locks (CanNotDelete) are applied to production resource groups to prevent accidental deletion

6. Platform Architecture Security

The Halved platform uses a two-service architecture: a Next.js web application (frontend and BFF layer) and a Python/FastAPI AI backend. These are deployed as separate Azure App Services and communicate via authenticated API calls.

**API security: **all requests from the web application to the AI backend require a valid API key. API routes in the frontend act as a proxy layer, preventing direct browser access to the AI backend.

**Service isolation: **the frontend and backend services run in separate App Service environments. The backend is not directly accessible from the public internet.

**Secrets management: **all secrets are stored in Azure Key Vault and referenced in application settings via Key Vault references. No secrets are stored in environment files or version control.

**FTPS: **FTP is disabled on production App Services. HTTPS is enforced on all production endpoints.

7. Monitoring and Auditing

Application logs from both production App Services are ingested into Azure Log Analytics Workspace (UK South) with 30-day retention

Deployment activity is tracked via GitHub Actions audit logs

Regular reviews of access logs and security configurations are conducted to identify anomalies

Resource-level audit logs are available through Azure Monitor

8. Incident Response

In the event of a security incident, an incident response process will be activated to assess the situation, contain any breach, and mitigate damage. A post-incident review will be conducted to analyse the cause and improve future responses. The incident response plan includes explicit reference to UK GDPR Article 33 (72-hour notification to ICO) and Article 34 (notification to data subjects) obligations. The CEO (Andrew James) is the named contact responsible for making regulatory notifications.

Where Halved acts as processor for a school, Halved must act in accordance with the provisions set out within any agreed data processing agreement, which shall include obligations to notify the school without undue delay after becoming aware of a personal data breach, provide information reasonably required by the school to assess notification obligations, and assist the school with any ICO or data subject notifications or security incident related activities.

9. Compliance and Best Practices

Halved is committed to compliance with UK GDPR and relevant data protection legislation. We regularly review industry best practices and update our security measures accordingly, including:

Reviewing dependency and package security in the CI/CD pipeline

Applying security patches and updates to platform dependencies

Annual review of this policy and associated controls

10. Training and Awareness

Halved team members with access to production systems receive guidance on security best practices, including secure coding, data handling procedures, and social engineering awareness. Halved also conduct periodic data protection training for all employees and staff to meet its obligations under data protection legislation.

11. Review and Updates

This Security Policy will be reviewed annually, or as required following changes in technology, platform architecture, or regulatory requirements. Updates will be communicated to relevant stakeholders. The next scheduled review is June 2027.

**Approved by: **Andrew James, CEO, Halved Limited | May 2026

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