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