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