



Kloodle Hub

Learner passport and evidence platform

SECURITY

Safeguarding and Data Security Overview

Version 1.2 · September 2026

**HOW WE PROTECT YOUR LEARNERS' DATA**

Safeguarding and data security

A plain-language overview for DSLs, heads and data protection leads

Kloodle Hub holds some of the most sensitive information a setting has: learner records, evidence of daily progress and, where enabled, safeguarding records. This overview explains how that information is protected. It accompanies our Data Processing Agreement, which sets out the formal commitments.

72h

maximum time to notify you of a personal data breach

1

setting per record: strict tenant isolation

TLS

encryption in transit; encrypted at rest by our hosts

100%

of safeguarding activity in an append-only audit log

Access is checked on every request

Your setting's data belongs to your setting alone. The database refuses direct access from browsers and apps; every read and write passes through the application server, which checks who is asking, what role they hold and which setting they belong to before anything is returned. Database row-level security adds a second, independent layer of the same rule.

Safeguarding records are held to a higher bar

Role-gated access

Safeguarding records are visible only to staff granted a safeguarding role, such as the DSL. Other staff cannot browse them, whatever their other permissions.

Confidential cases

Cases marked confidential are further restricted to the most senior safeguarding role only.

Append-only audit trail

Every action on a safeguarding record is written to an audit log that cannot be edited or deleted, preserving a trustworthy chronology for inspection.

Nothing hard-deleted

Safeguarding records are soft-deleted only, with the reason logged, so the evidential chain is never broken. Retention follows statutory guidance and your own policy.

Where your data lives

Kloodle Hub runs on established cloud infrastructure: Supabase (database and authentication, hosted in London, United Kingdom), Vercel (application hosting, with compute in London), Cloudflare R2 (file and evidence storage) and Resend (email delivery). Data is encrypted in transit using TLS and encrypted at rest by these providers, and databases are covered by automated backups. Our Data Processing Agreement lists each provider, where it processes data, and the safeguards applied.

AI features are optional and never see safeguarding records



Some reporting features use AI, provided by Anthropic, to help staff turn the evidence they have recorded into narrative reports and to read documents you upload. Three rules apply. Safeguarding module records are never sent to an AI provider. Any redaction list your setting configures is applied before anything is sent. And Anthropic is contractually barred from using your data to train its models. If you prefer, we will switch AI features off for your setting entirely, so no learner data is processed by AI at all.

Our commitments to you

We act only as a processor of your learners' data, on your instructions, under a written UK GDPR Article 28 agreement. We tell you without undue delay, and in any event within 72 hours, if a personal data breach affects your data. When a subscription ends you can export everything, and we then delete your data. We never sell personal data, and we never use learner data for advertising.

Where to go next

Questions, or want the formal detail? The Data Processing Agreement, Licence Agreement and Privacy Notice are available at kloodlehub.com/trust, or from Andrew Donnelly at andrew@kloodle.com.