



Kloodle Hub

Learner passport and evidence platform

DATA PROTECTION

Data Processing Agreement

Version 1.2 · September 2026

**UK GDPR ARTICLE 28**

Data Processing Agreement

How Kloodle Ltd processes personal data on behalf of your setting

1. Parties and scope

This Data Processing Agreement (the "DPA") forms part of the agreement between Kloodle Ltd, a company registered in England and Wales with company number 08497166, whose registered office is at Fold House, 3 Gregory Fold, Helmshore, Rossendale BB4 4JW, United Kingdom ("Kloodle", the "Processor"), and the customer named in the applicable Kloodle Hub order, quote or invoice (the "Customer", the "Controller").

It applies whenever Kloodle processes personal data on the Customer's behalf in the course of providing the Kloodle Hub platform and related services (the "Services"). It is entered into in accordance with Article 28 of the UK GDPR and the Data Protection Act 2018.

2. Roles of the parties

The Customer is the controller of the personal data of its learners, staff and other individuals that it (or they) enter onto the platform (the "Customer Personal Data"). Kloodle acts only as a processor of the Customer Personal Data, on the Customer's documented instructions.

Kloodle is an independent controller of its own business records, such as the contact and billing details of the Customer's staff who deal with Kloodle. That processing is described in the Kloodle Hub Privacy Notice.

3. Details of the processing

Item	Description
Subject matter	Provision of the Kloodle Hub learner passport and evidence platform.
Duration	The subscription term, plus the deletion period in clause 10.
Nature and purpose	Hosting, storage, display, reporting and secure sharing of learner records.
Data subjects	Learners (including children), staff, and employer contacts where used.
Personal data	Names, dates of birth, year group, contact details, photographs, evidence uploads, activity and attendance records, targets and reports.
Special category data	Where the safeguarding module is enabled, safeguarding records may include health and welfare information, processed to support the Customer's statutory safeguarding obligations.



4. Kloodle's obligations as processor

Kloodle shall: (a) process Customer Personal Data only on the Customer's documented instructions, including as set out in this DPA and the agreement, unless required to do otherwise by law, in which case Kloodle will inform the Customer unless the law prevents it; (b) ensure that all personnel authorised to process Customer Personal Data are bound by obligations of confidentiality; (c) implement and maintain the technical and organisational measures set out in Annex A; (d) taking into account the nature of the processing, assist the Customer in responding to requests from data subjects exercising their rights under the UK GDPR; (e) assist the Customer in meeting its obligations in relation to security, breach notification, and data protection impact assessments; (f) at the Customer's choice, delete or return Customer Personal Data at the end of the Services as set out in clause 10; and (g) make available to the Customer the information reasonably necessary to demonstrate compliance with this DPA, and allow for and contribute to audits conducted by the Customer or its appointed auditor, on reasonable notice and no more than once in any 12 month period.

5. Security

Kloodle implements appropriate technical and organisational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, as described in Annex A. These measures are reviewed and updated as the platform develops; Kloodle will not materially reduce the overall level of protection during the subscription term.

6. Sub-processors

The Customer gives general written authorisation for Kloodle to engage the sub-processors listed in Annex B. Kloodle will give the Customer at least 30 days' written notice of any intended addition or replacement, giving the Customer the opportunity to object on reasonable grounds relating to data protection. Kloodle imposes data protection obligations on each sub-processor equivalent to those in this DPA and remains responsible to the Customer for their performance.

7. AI-assisted features

Certain optional platform features use artificial intelligence to help staff turn recorded evidence into narrative reports, and to read documents the Customer uploads (for example baseline assessment reports). These features are provided through Anthropic, PBC, listed in Annex B. Only the information needed for the specific output is sent, any redaction list configured by the Customer's setting is applied before sending, and records held in the safeguarding module are never sent to any AI provider.

Anthropic is contractually prohibited from using Customer Personal Data to train its models. On request, Kloodle will disable AI-assisted features for the Customer's setting entirely, in which case no Customer Personal Data is processed by any AI provider. A United Kingdom-only AI processing option (Anthropic models served through AWS in London) is also available on request.

8. International transfers

Customer Personal Data is stored in the United Kingdom (London). Certain sub-processors listed in Annex B process limited categories of data in the United States or on global networks, as set out in that annex. Kloodle shall not transfer Customer Personal Data outside the UK unless the transfer is covered by UK adequacy regulations or by appropriate safeguards under Articles 46 to 49 of the UK GDPR (such as the ICO's International Data Transfer Agreement or Addendum), and will provide details of the safeguards relied on for each sub-processor on request.



9. Personal data breaches

Kloodle shall notify the Customer without undue delay, and in any event within 72 hours, after becoming aware of a personal data breach affecting Customer Personal Data. The notification will describe, so far as then known, the nature of the breach, the categories and approximate numbers of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address it. Kloodle will cooperate with the Customer and take reasonable steps to mitigate the effects of the breach.

10. Deletion and return of data

On termination or expiry of the Services the Customer may export its data from the platform, and Kloodle will provide reasonable assistance with export for 30 days after termination. Unless the law requires longer retention, Kloodle will delete all Customer Personal Data (including copies held by sub-processors) within 90 days of termination. Safeguarding and child protection records are the Customer's statutory responsibility; the Customer must export any records it is required to retain before deletion takes place.

11. General

This DPA takes effect from the subscription start date and continues for as long as Kloodle processes Customer Personal Data. It is subject to the limitations of liability in the main agreement between the parties. If there is a conflict between this DPA and the main agreement in relation to the processing of personal data, this DPA prevails. This DPA is governed by the law of England and Wales.

Signatures

Signed for and on behalf of Kloodle Ltd:

Name: Andrew Donnelly Position: Director Signature: _____ Date: _____

Signed for and on behalf of the Customer:

Name: _____ Position: _____ Signature: _____ Date: _____

Where the Customer accepts a Kloodle Hub order, quote or invoice that incorporates this document by reference, this document applies from the subscription start date whether or not it is separately signed.

**ANNEX A**

Technical and organisational measures

The safeguards applied to all customer data on Kloodle Hub

Tenant isolation

Every record on the platform belongs to a single setting. Access checks are enforced on every request so one setting can never see another setting's data.

Deny-by-default access control

The database refuses direct client access. All access is mediated by the application server, which checks the caller's identity, role and setting on every read and write. Database row-level security provides defence in depth.

Encryption

All data is encrypted in transit using TLS. Data is encrypted at rest by our hosting providers.

Role-based permissions

Staff, learner and employer accounts see only what their role allows. Safeguarding records carry additional role gates restricted to designated safeguarding staff.

Audit trail

Safeguarding records use an append-only audit log recording who did what and when. Records are soft-deleted only, preserving the evidential chain.

Authentication

Accounts are managed through the platform's authentication service with securely hashed credentials. Admin access to production systems is limited to named individuals on a least-privilege basis.

Backups and resilience

Databases are covered by provider-managed automated backups, supporting recovery in the event of accidental loss or corruption.

Secure development

Changes are version-controlled and reviewed before deployment. Security measures are re-assessed as new features (such as the safeguarding module) are added.



ANNEX B

Approved sub-processors

Third parties engaged by Kloodle to help deliver the platform

Sub-processor	Service provided
Supabase, Inc.	Database, authentication and application data hosting
Vercel, Inc.	Application hosting and content delivery
Cloudflare, Inc.	File and evidence storage (R2 object storage)
Resend, Inc.	Transactional email delivery (noreply@kloodlehub.com)
Anthropic, PBC	AI-assisted reporting and document reading (optional, see clause 7; can be disabled per setting)

Processing locations and transfer safeguards

Sub-processor	Where the data is processed
Supabase	London, United Kingdom (AWS eu-west-2). Primary store of all customer personal data, including safeguarding records.
Vercel	Serverless compute in London (lhr1); static site content is served from Vercel's global edge network.
Cloudflare	R2 object storage on Cloudflare's network, encrypted at rest.
Resend	United States (transactional email content only).
Anthropic	United States. Never receives safeguarding module records; contractually barred from training models on customer data.

Where a sub-processor processes personal data outside the United Kingdom, the transfer is covered by UK adequacy regulations or by the UK International Data Transfer Agreement or Addendum to the EU Standard Contractual Clauses, as set out in clause 8. Details of the safeguards relied on for each sub-processor are available in writing from andrew@kloodle.com.

Changes to this list are notified to customers at least 30 days in advance, as set out in clause 6 of the DPA.