



PROCUREMENT PACK

Data Processing Agreement

The terms on which Acarise Ltd processes personal data on behalf of a school, college or multi-academy trust, under Article 28 of the UK GDPR.

VERSION

1.0 draft

PREPARED

23 September 2026

CONTROLLER

The school, college or trust

PROCESSOR

Acarise Ltd

GOVERNING LAW

England and Wales

STATUS

Not yet legally reviewed

STATUS OF THIS DRAFT

This document has been drafted against the product as it actually works and against the real sub-processor list, but it has not been reviewed by a solicitor. It should not be offered for signature until it has been.

The parties

Controller	The school, college or multi-academy trust named in the Principal Agreement ("the School").
Processor	Acarise Ltd, company number 16831261, 283 Uxbridge Road, London W12 9DT ("Acarise").
Principal Agreement	The subscription or licence agreement between the parties for the Acarise platform.

This Agreement is incorporated into the Principal Agreement and takes effect on the same date. Where it conflicts with the Principal Agreement on the processing of personal data, this Agreement prevails.

Terms

1. Roles.

- 1.1 The School is the controller and Acarise is the processor in respect of the personal data described in Annex 1.
- 1.2 Acarise is an independent controller in respect of the School's staff account data, billing data, and Acarise's own records of how the service is used. That processing is governed by the Acarise Privacy Policy and not by this Agreement.
- 1.3 Each party is responsible for its own compliance with the UK GDPR and the Data Protection Act 2018.

2. Instructions.

- 2.1 Acarise processes the personal data only on the School's documented instructions, which are those in this Agreement, in the Principal Agreement, and as given through the ordinary use of the platform by the School's staff.
- 2.2 Acarise tells the School if it considers an instruction to breach data protection law, and may pause that processing until the instruction is withdrawn or amended.
- 2.3 Where Acarise is required by law to process the data otherwise, it tells the School first unless the law forbids it.

3. Confidentiality.

Acarise ensures that everyone authorised to process the personal data is bound by an obligation of confidentiality, and that access is limited to those who need it to operate, support or repair the service.

4. Security.

- 4.1 Acarise implements the technical and organisational measures set out in Annex 3, which the parties agree are appropriate to the risk having regard to the state of the art, the cost of implementation, and the nature, scope, context and purposes of the processing.
- 4.2 Acarise may update those measures provided the level of protection is not reduced.

5. Sub-processors.

- 5.1 The School gives general written authorisation for Acarise to engage the sub-processors listed in Annex 2.
- 5.2 Acarise gives the School at least 30 days' notice before adding or replacing a sub-processor. The School may object on reasonable data protection grounds within that period, and if the parties cannot resolve the objection the School may terminate the Principal Agreement without penalty in respect of the affected service.
- 5.3 Acarise imposes on each sub-processor obligations no less protective than those in this Agreement, and remains fully liable to the School for each sub-processor's performance.

- 6. International transfers.** Where personal data is transferred outside the United Kingdom, Acarise ensures an appropriate transfer mechanism is in place — the UK International Data Transfer Agreement, or the UK Addendum to the European Commission's Standard Contractual Clauses, or a UK adequacy decision. Annex 2 records where each sub-processor is located.
- 7. Data subject rights.**
 - 7.1 Acarise assists the School, by appropriate technical and organisational measures and so far as is reasonably possible, to respond to requests from data subjects exercising their rights.
 - 7.2 Where a data subject sends a request directly to Acarise, Acarise passes it to the School without undue delay and does not respond to it itself except to acknowledge it and say who to contact.
 - 7.3 The platform allows the School's staff to export a student's conversation as a text file at any time, without needing to contact Acarise.
- 8. Personal data breaches.**
 - 8.1 Acarise notifies the School without undue delay, and in any event within 48 hours, of becoming aware of a personal data breach affecting the personal data.
 - 8.2 The notification describes the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, the measures taken or proposed, and a contact point.
 - 8.3 Acarise assists the School in meeting its own obligations under Articles 33 and 34.
- 9. Data protection impact assessments.** Acarise provides the School with the information it reasonably needs to carry out a data protection impact assessment and, where required, to consult the Information Commissioner. The Acarise DPIA Information Pack is provided for this purpose.

10. Deletion and return.

- 10.1 On termination of the Principal Agreement, and at the School's choice, Acarise deletes or returns the personal data.
- 10.2 Unless the School instructs otherwise, personal data is deleted 12 months after termination. The School may request deletion sooner, and Acarise will carry it out within 30 days of the request.
- 10.3 Acarise may retain personal data where UK law requires it, and in that case continues to protect it under this Agreement.
- 10.4 Acarise confirms deletion in writing on request.

11. Audit.

- 11.1 Acarise makes available to the School the information necessary to demonstrate compliance with Article 28.
- 11.2 Acarise allows for and contributes to audits, including inspections, conducted by the School or an auditor it mandates, on reasonable notice, no more than once in any twelve-month period except following a personal data breach, and subject to confidentiality.

12. Duration. This Agreement applies for as long as Acarise processes personal data on the School's behalf, and the obligations in clauses 3, 10 and 11 survive its termination.

13. Governing law. This Agreement is governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction.

Annex 1 — What is processed

Subject matter	Provision of the Acarise learning platform to the School's staff and students.
Duration	The term of the Principal Agreement, plus the retention periods in clause 10.
Nature and purpose	Hosting and storage; generating learning activities from a teacher's objective; conducting a written conversation between a student and an AI tutor; assessing progress against learning objectives; generating and scoring quizzes; reporting progress to the student's teacher.
Categories of data subject	Students, and the School's teaching and administrative staff.

TYPES OF PERSONAL DATA

Data subject	Data
Students	Name; email address; hashed sign-in passphrase; the full text of conversations with the AI tutor; quiz answers and scores; progress and confidence recorded against each learning objective; group and activity membership; session timestamps.
Staff	First and last name; email address; hashed password; the groups, activities and settings they create; feedback they submit.
Technical	IP address, device and browser information, and error records, in server logs.

SPECIAL CATEGORY DATA

Acarise does not ask for special category data, and none of its fields are designed to hold any. A student writing freely to the AI tutor could nonetheless disclose it. The School should account for that possibility in its own DPIA.

Annex 2 — Sub-processors

Sub-processor	Purpose	Personal data	Location
Vercel Inc.	Application hosting and delivery	All data in transit; server logs; IP addresses	US
Supabase Inc.	Database and authentication	All stored data	EU
OpenAI	AI models for the tutor, the progress analyser, and activity and quiz generation	Conversation and activity content, per request	US
Langfuse	Recording AI requests for quality monitoring and fault diagnosis	Copies of text sent to and returned from the AI, including student messages	EU
Resend	Transactional email	Name and email address	US
Vercel Analytics	Aggregate page view counts	No personal data; no cookies	US

Under the agreement in force with OpenAI, content submitted through the API is not used to train its models.

Annex 3 — Technical and organisational measures

Set out in full in the Acarise Information Security Overview, which forms part of this Annex. In summary:

Area	Measure
Encryption	Data encrypted in transit (TLS) and at rest by the hosting and database providers.
Access control	Roles assigned server-side and unchangeable from a browser. Educator screens and APIs closed to students. An action on a student is permitted only to an educator whose group that student is in.
Database isolation	Row-level security policies restrict access at the database layer.
Credentials	Passwords and passphrases stored hashed; never held in readable form.
Assessment integrity	Quiz answer keys held server-side and never serialised to a browser.
Account provisioning	Educator accounts approved individually by an Acarise administrator.
Monitoring	AI requests traced; application errors recorded and reviewed.
Staff access	Limited to what is needed to operate, support or repair the service; not browsed routinely.

Signature

For the School	For Acarise Ltd
Name	Name
Position	Position
Date	Date
Signature	Signature

Acarise Ltd · 283 Uxbridge Road, London W12 9DT · Company No. 16831261, registered in England and Wales · contact@acarise.com