



A product of



ClassPilot Data Processing Agreement

Version 0.2 | 19 September 2026

Including the UK GDPR Article 28 processing schedule

Agreement overview

This Data Processing Agreement forms part of the agreement under which the school or academy trust uses ClassPilot. It sets out the terms on which Edapt Technologies processes personal data on the school's behalf and is intended to satisfy the requirements applying to controller and processor contracts under Article 28 of the UK GDPR.

The controller is the school or academy trust identified in the applicable Order Form, trial agreement or subscription agreement. The processor is David Edmonds trading as Edapt Technologies. The parties' correspondence addresses are those stated in the applicable Order Form or main agreement.

If this Data Processing Agreement conflicts with the main agreement on the protection or processing of personal data, this Data Processing Agreement takes priority to the extent of that conflict. The schedules form part of this agreement.

1 Definitions

In this agreement, Controller, Data Subject, Personal Data, Personal Data Breach, Processing and Processor have the meanings given to them in applicable UK data protection law.

Applicable Data Protection Law means the UK GDPR, the Data Protection Act 2018, relevant provisions of the Data Use and Access Act 2025, and other binding UK laws governing the processing covered by this agreement, as amended from time to time.

Main Agreement means the Order Form, trial agreement, subscription agreement or other written agreement under which the Controller receives ClassPilot. Subprocessor means another processor engaged by Edapt Technologies to process personal data for the Controller in connection with ClassPilot.

2 Roles and scope

The Controller determines the purposes and essential means of the processing. Edapt Technologies processes personal data only to provide, secure, support and maintain ClassPilot and otherwise as documented by the Controller.

The subject matter, duration, nature, purpose, data types and categories of Data Subject are described in Schedule 1. The Controller retains all rights and responsibilities that applicable law places on a controller.

3 Controller responsibilities

The Controller will:

- ensure that its processing through ClassPilot is lawful, fair and transparent and that it has identified an appropriate lawful basis and, where required, an Article 9 condition;

- provide required privacy information to pupils, staff, parents, carers and other affected people;
- give lawful, documented and sufficiently clear instructions to Edapt Technologies;
- ensure that personal data supplied to ClassPilot is relevant, accurate, limited to what is necessary and collected lawfully;
- authorise users appropriately, maintain accurate role assignments and promptly remove access that is no longer required;
- avoid entering safeguarding records, home addresses, parent contact details or unrelated sensitive information into free-text fields; and
- involve its data protection officer or data protection lead when required, including for DPIAs and decisions about AI-assisted processing.

4 Documented instructions

Edapt Technologies will process personal data only on the Controller's documented instructions, including instructions contained in the Main Agreement, this Data Processing Agreement, authorised use of ClassPilot and written support requests.

Edapt Technologies will not process personal data for its own unrelated purposes, sell it, use it for advertising, or use pupil information to train generative AI foundation models.

If Edapt Technologies believes an instruction infringes Applicable Data Protection Law, it will inform the Controller without undue delay and may suspend the affected processing until the parties agree a lawful instruction. Edapt Technologies may process personal data where UK law requires it to do so, but will notify the Controller before that processing unless the law prohibits notification.

5 Confidentiality and authorised personnel

Edapt Technologies will restrict access to personal data to people who need it to provide, secure or support ClassPilot. Any employee, contractor or other authorised person with access will be subject to an appropriate duty of confidentiality and relevant data protection and security responsibilities.

Edapt Technologies will ensure that access is removed or changed promptly when a person's responsibilities end or change.

6 Security of processing

Taking account of the state of the art, implementation cost, the nature, scope, context and purposes of processing, and the risks to individuals, Edapt Technologies will maintain appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

The current categories of measure are set out in Schedule 2. Edapt Technologies may update individual measures as technology and risk change, provided that the overall level of protection is not materially reduced.

The Controller remains responsible for the security of its users, devices, networks, identity systems, exports and any copies of ClassPilot information held outside the service.

7 Subprocessors

The Controller gives general written authorisation for Edapt Technologies to use the subprocessors listed in Schedule 3. Edapt Technologies will enter into written terms with each subprocessor that impose data protection obligations offering an appropriate level of protection for the processing concerned.

Edapt Technologies will remain responsible to the Controller for the performance of its subprocessors' data protection obligations as required by Applicable Data Protection Law.

Edapt Technologies will give the Controller at least 30 days' notice before adding or replacing a subprocessor that will process school personal data, except where urgent action is reasonably required to maintain security or service continuity. The Controller may object on reasonable data protection grounds within 14 days of notice. The parties will work in good faith to resolve the concern. If no reasonable resolution is available, either party may terminate the materially affected service in accordance with the Main Agreement.

8 International transfers

Edapt Technologies will make a restricted international transfer only on the Controller's documented instructions (unless UK law requires otherwise) and where a valid legal transfer route under Applicable Data Protection Law is in place. Controller instructions alone do not authorise an otherwise unlawful transfer.

The core ClassPilot application and database are configured in Microsoft Azure UK South. Processing location for Azure OpenAI depends on the selected model deployment type and configuration and must be confirmed before live school onboarding. Where a restricted transfer occurs, the parties will rely on an applicable adequacy regulation, the UK International Data Transfer Agreement, the UK Addendum to approved contractual clauses or another legally recognised safeguard, together with supplementary measures where required.

9 Data Subject requests

Taking account of the nature of the processing, Edapt Technologies will provide reasonable technical and organisational assistance to enable the Controller to respond to requests to exercise Data Subject rights.

If Edapt Technologies receives a request relating to school-controlled data, it will not respond substantively unless authorised by the Controller or required by law. It will forward the request to the Controller without undue delay where the requester can be identified as connected with that Controller.

The Controller is responsible for deciding whether and how a request should be fulfilled. Additional work outside the service's standard export and administration functions may be charged at a reasonable rate where permitted by law and agreed in advance, except where the assistance is required because of Edapt Technologies' breach of this agreement.

10 Personal Data Breaches

Edapt Technologies will notify the Controller without undue delay after becoming aware of a Personal Data Breach affecting the Controller's personal data. Where practicable, an initial notification will be made within 24 hours of awareness, with further information supplied in phases as it becomes available. Investigation or formal confirmation must not delay a notification required by law.

The notification will, to the extent then known, describe the nature of the breach, the categories and approximate number of affected individuals and records, likely consequences, measures taken or proposed, and a contact point for further information.

Edapt Technologies will take reasonable steps to contain, investigate and mitigate the breach, preserve relevant evidence and assist the Controller with its assessment and any required notification. The Controller remains responsible for deciding whether to notify the Information Commissioner's Office or affected individuals unless the law provides otherwise.

11 Compliance assistance

Taking account of the nature of processing and the information available to it, Edapt Technologies will provide reasonable assistance with the Controller's obligations concerning security, breach assessment and notification, Data Protection Impact Assessments and prior consultation with the Information Commissioner's Office.

Edapt Technologies will make available information reasonably necessary to demonstrate compliance with the processor obligations covered by this agreement. The Controller should use supplied policies, assurance information and independent reports before requesting a bespoke audit.

12 Audits and inspections

The Controller may audit Edapt Technologies' compliance with this agreement no more than once in any 12-month period, unless a material security incident, credible evidence of non-compliance or a regulator reasonably requires an additional audit.

An audit must be proportionate, limited to processing relevant to the Controller, conducted during normal working hours on at least 20 working days' notice where circumstances permit, and arranged to protect other customers, confidential information and system security. Remote evidence review will be used where it can provide reasonable assurance.

The Controller will bear its audit costs and Edapt Technologies' reasonable costs of unusual or extensive assistance unless the audit identifies a material breach by Edapt Technologies, in which case Edapt Technologies will bear its own reasonable remediation and assistance costs.

13 Return and deletion

At the end of the service, the Controller may choose return followed by deletion, or deletion without return, of all school-controlled personal data. The parties will agree a secure and usable return method covering the full dataset, including any data not included in a standard export. Edapt Technologies will delete existing copies unless UK law requires their storage, subject to the protected backup-expiry process below.

Unless the Controller lawfully instructs otherwise, Edapt Technologies will delete school-controlled personal data from active systems within 30 days after termination of the affected service. Residual encrypted copies may remain temporarily in backups until overwritten through the configured backup cycle and will remain protected and unavailable for routine use.

Any exception to deletion of school-controlled personal data must be based on a UK legal storage requirement, limited to the necessary information and duration, and communicated to the Controller unless prohibited by law. Separate business-contact, contract and financial records for which Edapt Technologies acts as controller follow the Service Privacy Notice; this does not authorise retaining pupil records for general business, audit or legal-rights purposes.

14 Changes in law or processing

The parties will cooperate in good faith to amend this agreement where a change in law, regulatory guidance, ClassPilot functionality or processing arrangements makes an amendment reasonably necessary. Edapt Technologies will give reasonable notice of a material change where practicable.

A material new category of personal data, new purpose, significant AI use or new international transfer arrangement will be assessed before implementation and reflected in the relevant schedule and privacy information.

15 Liability

Each party is responsible for its own compliance with Applicable Data Protection Law. Liability arising under this agreement is subject to the exclusions, limitations and allocation of liability in the Main Agreement, except to the extent that Applicable Data Protection Law prevents such limitation.

Nothing in this agreement limits a Data Subject's rights or either party's liability to a supervisory authority where that liability cannot lawfully be limited.

16 Term and termination

This agreement begins when it is incorporated into the Main Agreement and continues while Edapt Technologies processes personal data for the Controller. Provisions intended by their nature to continue, including confidentiality, security, deletion, audit cooperation and liability, survive termination for as long as relevant personal data remains in Edapt Technologies' possession or control.

17 Notices and governing law

Operational and data protection notices to Edapt Technologies must be sent to support@edapt-tech.co.uk. Notices to the Controller will be sent to the authorised contact recorded in the Main Agreement or ClassPilot administration records.

This agreement and any non-contractual obligations arising from it are governed by the law of England and Wales. The courts of England and Wales have jurisdiction, subject to any mandatory legal rights or public-law requirements applying to the Controller.

Schedule 1 Processing details

Requirement	ClassPilot processing
Subject matter	Provision of a school assessment, progress analysis and reporting service, including authorised AI-assisted report drafting.
Duration	For the term of the Main Agreement, followed by the agreed export and deletion period and temporary expiry of residual encrypted backups.
Nature of processing	Collection from the Controller, recording, organisation, storage, retrieval, consultation, calculation, display, use, AI inferencing where selected, report generation, review, export, restriction, archiving and deletion.
Purposes	School setup; user administration; pupil and class management; assessment recording; age-related expectation and progress analysis; reporting; school-authorised AI drafting; security; audit; support; maintenance; export and offboarding.
Frequency	Ongoing and event-driven during authorised use of ClassPilot.
Data Subjects	Pupils; authorised school and trust staff; school contacts; and, only where included by an authorised user in relevant report content, parents or carers.

Requirement	ClassPilot processing
Pupil personal data	First name, surname, unique pupil number, school, class, year group, learning groups, subject and assessment records, scores, teacher judgements, age-related expectation information, progress indicators, comments, report drafts, approved reports, review information, archive status and audit references.
Staff and account data	Name, work email, school, role, assigned classes, permission scope, authentication identifiers, account and invitation status, session and security information, audit events, support records and relevant technical data.
Special category data	SEN status and details, and any health, disability, ethnic-origin or other special category information contained within school-authorised educational records. EAL status may also be processed but does not by itself necessarily constitute special category data.
Excluded standard data	ClassPilot does not require date of birth, home address, parent contact details, attendance history or safeguarding records as part of the standard dataset.
AI prompt data	A pupil's name, relevant assessment or judgement information, teacher-provided context and report text may be processed when an authorised user requests drafting. UPN is not intended to be included in AI prompts.
Retention	For the service term, subject to Controller instructions; active-system deletion within 30 days after termination; residual backups protected until expiry under the agreed schedule. Exceptions for school-controlled data are limited to UK legal storage requirements. Separate controller business records follow the Service Privacy Notice.

Schedule 2 Technical and organisational measures

Control area	Current measures
Hosting and physical security	Core application and database services use Microsoft Azure UK South and inherit relevant Azure datacentre and platform controls.
Encryption	HTTPS and TLS protect supported data connections in transit. Azure platform encryption protects supported data at rest. Database connections require SSL.
Secrets management	Production secrets are held in Azure Key Vault or protected application configuration and are not committed to source code.
Authentication	Access is invite-only. Supported sign-in methods use protected session handling, secure cookies and inactivity controls. Invitation tokens are stored in hashed form.

Control area	Current measures
Access control	School, role, profile and class scopes restrict access. Server-side authorisation and school-isolation checks are used for protected data operations.
Tenant separation	School identifiers and enforced authorisation boundaries are used to prevent access across school environments. Isolation and permission behaviour form part of automated testing.
Audit and accountability	Relevant authentication, data-change, workflow, export and administrative events are recorded where supported to assist accountability and investigation.
Availability and recovery	Azure service resilience and configured database backup capabilities support continuity and recovery. Backup and restore arrangements will be recorded and tested as production operations mature.
Secure development	Source control, separated environments, dependency management, schema migrations, linting, automated tests, production builds and controlled deployment workflows support change assurance.
Incident management	Suspected incidents are assessed, contained, documented and escalated. Controller notification and cooperation follow clause 10.
Personnel and confidentiality	Access is limited to authorised personnel with a business need. Contractors or advisers receiving personal data must be subject to suitable confidentiality and data protection terms.
Data minimisation	The standard dataset excludes unnecessary contact, attendance and safeguarding data. Users are instructed not to place unrelated sensitive information in free-text fields.
AI safeguards	AI drafting is user-initiated, limited to the report-writing purpose and subject to teacher review. Azure-hosted prompts and outputs are not used to train generative foundation models without permission or instruction.

Schedule 3 Approved subprocessors

Subprocessor	Services	Processing and location position
Microsoft	Microsoft Azure and Microsoft Azure OpenAI	Azure provides application hosting, database, networking, secrets, security, logging, backup and related infrastructure; core ClassPilot resources are configured in UK South. Azure OpenAI processes selected prompt content and returns AI-assisted report wording. The AI deployment type, precise processing geography and abuse-monitoring configuration must be confirmed before live onboarding. Microsoft's applicable data protection terms and transfer safeguards apply.

Edapt Technologies will update this schedule before appointing another subprocessor to handle school personal data and will follow the notice and objection process in clause 7.

Schedule 4 Operational contacts

Purpose	Contact route
Privacy and Data Subject support	support@edapt-tech.co.uk
Security incidents and suspected breaches	support@edapt-tech.co.uk with the subject line Urgent Security Incident
Subprocessor notices	The authorised school contact recorded in the Main Agreement or ClassPilot administration records
Formal correspondence	The addresses stated in the applicable Order Form or Main Agreement

Document status

Version 0.2 is a working draft prepared for operational review and professional legal validation. It should not be treated as executed until incorporated into an accepted Main Agreement. The Azure OpenAI deployment type, processing geography and abuse-monitoring position must be verified before the first live school onboarding.