Data Processing Agreement

Last updated 1 July 2026

Made under Article 28 of the UK GDPR

This Data Processing Agreement (the **"Agreement"**) is entered into between:

(1) Polymorphic Studios Ltd, a company registered in England & Wales (company no. 09041072), whose registered office is at 237 Westcombe Hill, London, SE3 7DW, trading as **"Software for Schools"** (the **"Processor"**, **"we"**, **"us"**); and

(2) the customer identified in the Order Form (the **"Controller"**, the **"Customer"**, **"you"**),

each a **"Party"** and together the **"Parties"**.

Effective date: the date of the Order Form

1. Background and purpose

1.1 The Processor provides the software product or online service identified in the Order Form (the **"Service"**). The nature, scope and purpose of the processing carried out by the Processor through the Service on behalf of the Customer are described in **Annex 1**.

1.2 In providing the Service, the Processor processes personal data on behalf of the Customer, including personal data relating to children. The Customer is the controller of that personal data and the Processor is a processor.

1.3 This Agreement governs that processing and forms part of, and is subject to, the Terms of Service together with the Order Form (the **"Principal Agreement"**). Where this Agreement conflicts with the Principal Agreement on the subject of data protection, this Agreement prevails.

1.4 This Agreement is designed to satisfy the requirements of Article 28 of the UK GDPR.

2. Definitions

2.1 In this Agreement:

- **"Data Protection Law"** means all law applicable to the processing of personal data under this Agreement, including the UK GDPR, the Data Protection Act 2018, and any guidance or codes of practice issued by the Information Commissioner's Office (**"ICO"**).
- **"UK GDPR"** has the meaning given in section 3(10) of the Data Protection Act 2018.
- **"Personal Data"**, **"special category data"**, **"data subject"**, **"controller"**, **"processor"**, **"processing"**, **"personal data breach"** and **"supervisory authority"** each have the meaning given in Data Protection Law.
- **"Customer Personal Data"** means the Personal Data described in **Annex 1** that the Processor processes on behalf of the Customer under this Agreement.
- **"Sub-processor"** means any third party engaged by the Processor to process Customer Personal Data.

2.2 The terms of this Agreement are in addition to, and do not relieve, remove or replace, a Party's obligations or rights under Data Protection Law.

3. Roles of the Parties

3.1 The Parties acknowledge that, for the purposes of Data Protection Law, the Customer is the controller and the Processor is the processor in respect of the Customer Personal Data.

3.2 The Customer is responsible for establishing and maintaining a lawful basis for the processing of the Customer Personal Data, for issuing any privacy information to data subjects, and for obtaining any consents that may be required.

4. Processing of Customer Personal Data

4.1 The Processor shall process Customer Personal Data **only on the documented instructions of the Customer**, including with regard to international transfers, unless required to do otherwise by law (in which case, unless prohibited by law on important grounds of public interest, the Processor shall inform the Customer of that legal requirement before processing).

4.2 The Customer's documented instructions are set out in this Agreement (including Annex 1) and the Principal Agreement, as supplemented by the Customer's use and configuration of the Service. Additional instructions must be agreed in writing.

4.3 The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of data subject are described in **Annex 1**.

4.4 The Processor shall immediately inform the Customer if, in its opinion, an instruction infringes Data Protection Law.

4.5 The Processor shall not sell Customer Personal Data and shall not use it for its own purposes, for advertising or marketing to data subjects, or to train, develop or improve any artificial-intelligence or machine-learning model.

5. Confidentiality

5.1 The Processor shall ensure that any person authorised to process Customer Personal Data (including its staff) is subject to an appropriate duty of confidentiality and is made aware of the confidential nature of the data.

5.2 The Processor shall ensure that access to Customer Personal Data is limited to those personnel who need access to perform the Processor's obligations under the Principal Agreement.

5.3 The confidentiality obligations in this clause 5 continue in force after the termination or expiry of this Agreement.

6. Security

6.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk to data subjects, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in **Annex 2**.

6.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks presented by processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data. The Parties acknowledge that the Customer Personal Data relates primarily to children and shall therefore be handled with an appropriately high standard of care.

7. Sub-processors

7.1 The Customer provides **general written authorisation** for the Processor to engage Sub-processors to process Customer Personal Data, subject to this clause 7. The Sub-processors engaged at the effective date are listed in **Annex 3**.

7.2 The Processor shall inform the Customer of any intended addition or replacement of a Sub-processor at least **30 days** in advance, giving the Customer the opportunity to object on reasonable data-protection grounds. If the Customer reasonably objects and the Parties cannot resolve the objection, the Customer may suspend or terminate the affected part of the Service without penalty.

7.3 The Processor shall impose on each Sub-processor, by written contract, data-protection obligations that are no less protective than those in this Agreement. The Processor remains fully liable to the Customer for the performance of each Sub-processor's obligations.

8. International transfers

8.1 The Processor shall not transfer Customer Personal Data to a country outside the United Kingdom unless it has first taken such measures as are necessary to ensure the transfer is lawful under Data Protection Law — for example, that the destination is covered by UK adequacy regulations, or that an appropriate safeguard is in place such as the UK Extension to the EU–US Data Privacy Framework or the ICO's International Data Transfer Agreement / Standard Contractual Clauses (as applicable).

9. Assistance to the Customer

9.1 Taking into account the nature of the processing, the Processor shall assist the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling the Customer's obligation to respond to requests from data subjects exercising their rights under Data Protection Law (including access, rectification, erasure, restriction, portability and objection).

9.2 The Processor shall promptly notify the Customer if it receives a request from a data subject in relation to Customer Personal Data, and shall not respond to that request itself except on the Customer's documented instructions or as required by law.

9.3 Taking into account the nature of processing and the information available to it, the Processor shall assist the Customer in ensuring compliance with its obligations relating to security of processing, personal data breaches, data protection impact assessments, and prior consultation with the ICO (UK GDPR Articles 32 to 36).

9.4 The Processor shall notify the Customer without undue delay if it becomes aware that it can no longer comply with this Agreement or its obligations under applicable Data Protection Law.

10. Personal data breaches

10.1 The Processor shall notify the Customer **without undue delay, and in any event within 48 hours**, after becoming aware of a personal data breach affecting Customer Personal Data.

10.2 The notification shall, to the extent known, describe the nature of the breach (including the categories and approximate number of data subjects and records concerned), the likely consequences, and the measures taken or proposed to address it and mitigate its effects. Where the information is not all available at once, it may be provided in phases without undue further delay.

10.3 The Processor shall cooperate with the Customer and take such reasonable steps as the Customer directs to assist in the investigation, mitigation and remediation of the breach.

11. Audit and records

11.1 The Processor shall make available to the Customer all information necessary to demonstrate compliance with the obligations in Article 28 of the UK GDPR and this Agreement.

11.2 The Processor shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, on reasonable prior written notice and no more than once in any 12-month period (save where required following a personal data breach or by the ICO). The Processor may satisfy this obligation by providing relevant certifications, security documentation or third-party audit reports where these reasonably address the Customer's request. The Customer shall bear its own costs of any such audit, unless the audit identifies a material breach by the Processor, in which case the Processor shall reimburse the Customer for its reasonable and proportionate audit costs directly attributable to investigating that breach.

11.3 The Processor shall maintain a written record of its categories of processing activities carried out on behalf of the Customer, as required by Article 30(2) of the UK GDPR.

12. Return and deletion of data

12.1 On termination or expiry of the Principal Agreement, and at the choice of the Customer, the Processor shall **delete or return** all Customer Personal Data and delete existing copies, unless Data Protection Law requires continued storage. Deletion shall be carried out using secure deletion methods appropriate to the storage medium, where technically feasible.

12.2 The Processor shall make Customer Personal Data available for export by the Customer in a commonly used format during the term and for a period of **30 days** after termination, after which it shall be deleted in accordance with clause 12.1.

12.3 The Processor shall, on request, certify in writing to the Customer that it has complied with this clause 12. Backups containing Customer Personal Data are made inaccessible for operational use and are then overwritten or deleted in the ordinary course of the Processor's backup retention cycle.

13. Liability and term

13.1 Each Party's liability arising out of or in connection with this Agreement is subject to the limitations and exclusions of liability set out in the Principal Agreement.

13.2 This Agreement takes effect on the effective date and continues for as long as the Processor processes Customer Personal Data on behalf of the Customer. Clauses that by their nature should survive termination (including clauses 5, 12 and 13) shall do so.

14. General

14.1 This Agreement is governed by the laws of England and Wales, and the courts of England and Wales have exclusive jurisdiction.

14.2 If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

14.3 This Agreement may be executed in counterparts, including by electronic signature, each of which is an original and which together constitute one agreement.

Annex 1 — Details of the processing

Subject matter of the processing The provision of the Service identified in the Order Form to the Customer. The Service currently provides pupil assessment and progress-tracking functionality, enabling the Customer to record, organise and report on pupils' attainment against curriculum frameworks.

Duration of the processing For the term of the Principal Agreement, plus the limited retention period for return/deletion set out in clause 12.

Nature and purpose of the processing Hosting, storage, organisation, structuring, retrieval, display, analysis and reporting of pupil assessment information, and the administration of staff user accounts, so that the Customer can record and track pupils' attainment against curriculum frameworks. Processing is carried out by automated means within the Service.

Categories of data subject

- Pupils (children) whose data is processed by the Customer through the Service.
- Staff of the Customer who are users of the Service.

Types of Personal Data

Relating to pupils:

- Identifying information: first name and last name.
- Education/organisational information: class, year group / key stage, and curriculum framework groupings.
- Assessment information: attainment levels and judgements recorded against curriculum statements, by term.

- Free-text assessment notes entered by staff. These fields are controlled by the Customer and may, depending on what staff enter, contain further information about a pupil (potentially including special category data such as information relating to a pupil's health or special educational needs). The Customer is responsible for the content it enters and for any lawful basis / conditions required for such data.

Relating to staff users:

- Name and email address.
- Authentication data: hashed password and two-factor authentication settings.
- Technical/usage data generated by use of the Service: IP address, browser/user-agent, and activity/session logs.

Special category data The Service is not designed for the deliberate storage of special category data. Such data may nonetheless be present where staff enter it into free-text fields. Any such processing is on the documented instruction of, and under the control of, the Customer.

Frequency of the processing Continuous, for the duration of the Principal Agreement.

Annex 2 — Technical and organisational security measures

The Processor maintains the following measures, which it may update from time to time provided the level of security is not materially reduced:

Access control and authentication

- Role-based access controls, with each user's access scoped to their own school's data ("tenant isolation"); users cannot access data belonging to other schools.
- Support for two-factor authentication on staff accounts.
- Passwords stored only in hashed form using a strong, salted hashing algorithm.
- Access to production systems and data restricted to authorised personnel on a need-to-know basis.

Encryption

- Encryption of Customer Personal Data in transit using current TLS.
- Encryption of data at rest at the hosting/storage layer.

Hosting infrastructure

- Customer data is primarily hosted within the AWS London (eu-west-2) region in the United Kingdom.

Operational security

- Logically segregated environments and least-privilege administrative access.

- Access to Customer Personal Data for support or maintenance purposes is limited to authorised personnel, and only where necessary to investigate issues, provide support, or maintain the Service.
- Logging of significant actions within the Service to support accountability and investigation.
- Regular application of security updates to the application and its dependencies.

Resilience and backups

- Regular automated backups, with the ability to restore data in the event of an incident.
- Disaster recovery and business continuity procedures are maintained and tested periodically.
- Use of reputable cloud infrastructure providers offering high availability.

Organisational measures

- Confidentiality obligations for personnel with access to Customer Personal Data.
- Personnel with access to Customer Personal Data receive appropriate data protection and security awareness training.
- Sub-processors engaged under written contracts with equivalent data-protection obligations.
- A personal-data-breach notification process consistent with clause 10.

Annex 3 — Authorised Sub-processors

Sub-processor	Service provided	Location of processing	Safeguard for any transfer outside the UK
Laravel Cloud (Laravel Holdings Inc.), running on Amazon Web Services	Application and database hosting, infrastructure and backups	AWS London (eu-west-2)	Customer data is hosted within the AWS London (eu-west-2) region; appropriate international transfer safeguards are incorporated into the provider's DPA where applicable
Laravel Nightwatch (Laravel Holdings Inc.)	Application performance monitoring and error/observability telemetry (may incidentally include personal data present in requests, queries or exceptions)	Europe (Frankfurt)	Data processed within the EEA, which is covered by UK adequacy regulations; provider DPA applies
Postmark (AC PM, LLC, an ActiveCampaign company)	Transactional email (e.g. account, invitation, password-reset and notification emails)	United States	Provider DPA; UK Extension to the EU–US Data Privacy Framework and/or IDTA / SCCs
Cloudflare, Inc.	DNS, content delivery (CDN), and network security / WAF; site traffic (including IP addresses) is proxied through Cloudflare's edge network	Global edge network (including the UK); provider established in the United States	Provider DPA; UK Extension to the EU–US Data Privacy Framework and/or IDTA / SCCs

Sub-processor	Service provided	Location of processing	Safeguard for any transfer outside the UK
Fastmail Pty Ltd	Business email hosting (may incidentally include personal data present in correspondence)	United States (provider established in Australia)	Provider DPA incorporating the EU Standard Contractual Clauses (2021)
Docsketch, LLC (trading as SignWell)	Electronic signature of agreements (e.g. names, email addresses and signatures of signatories)	United States	Provider DPA; transfer made in reliance on its necessity for performance of the contract

A current list of Sub-processors is available to the Customer on request. The Processor will notify the Customer of changes in accordance with clause 7.