

Data Processing Agreement

Magma Maths | Radish Education UK Ltd

This Data Processing Agreement ("DPA") is made between the Controller and Radish Education UK Ltd, doing business as Magma Maths (the "Processor").

Radish AB is the Swedish parent company. Magma Maths is the service provided and operated by Radish Education UK Ltd.

1. Introduction and Precedence

This DPA forms part of the agreement between the parties for the provision of the Magma Maths service (the "Principal Agreement"). It governs the Processor's processing of personal data on behalf of the Controller and is designed to satisfy Article 28 of the UK GDPR.

Where there is any conflict or inconsistency between this DPA and the Processor's Terms of Use, the Principal Agreement, or any other terms published by the Processor, this DPA prevails in respect of the processing of personal data.

For the avoidance of doubt, any licence granted to the Processor in respect of user-created content under the Terms of Use, including without limitation the licence at clauses 3.6 and 3.7 of the Terms of Use as at the date of this DPA, does not apply to pupil-submitted content, pupil work, or any other personal data processed under this DPA. Such data is processed solely to deliver the Magma Maths service on the Controller's documented instructions. It is not used for any other purpose, including marketing, profiling, product development unrelated to service delivery, or the training or improvement of artificial intelligence models. This restriction continues to apply after the content is deleted and after this DPA terminates.

Liability between the parties is as set out in the Principal Agreement.

2. Definitions

- "Applicable Data Protection Law" means the UK GDPR, the Data Protection Act 2018, and any other data protection legislation applicable to the processing.
- "Controller" means the school, multi-academy trust, college, college group or local authority determining the purposes and means of the processing.
- "Processor" means Radish Education UK Ltd.
- "Personal Data" means any information relating to an identified or identifiable natural person processed under this DPA.
- "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.
- "Sub-processor" means any third party engaged by the Processor to process Personal Data on the Controller's behalf.
- "UK GDPR" means the Regulation as retained in UK law following the withdrawal of the United Kingdom from the European Union.

Terms not defined here have the meaning given in Applicable Data Protection Law.

3. Subject Matter, Duration and Purpose

The subject matter, duration, nature and purpose of the processing, the categories of data subject and the types of Personal Data are set out in Annex I.

Processing continues for the duration of the Controller's use of the Magma Maths service and ends when the Principal Agreement terminates and all Personal Data has been returned or deleted in accordance with Section 16.

4. Controller Instructions

The Processor shall process Personal Data only on the documented instructions of the Controller, including in relation to transfers of Personal Data to a third country, unless required to do otherwise by law. Where the Processor is required by law to process Personal Data otherwise than on the Controller's instructions, it shall inform the Controller of that legal requirement before processing, unless the law prohibits it from doing so on important grounds of public interest.

The Principal Agreement and this DPA constitute the Controller's complete documented instructions as at the date of this DPA. Further instructions may be issued in writing.

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

5. Processor Obligations

The Processor shall:

- Process Personal Data only as set out in Section 4.
- Implement and maintain the technical and organisational measures set out in Annex II.
- Ensure that persons authorised to process Personal Data are subject to an appropriate duty of confidentiality.
- Assist the Controller in responding to requests from data subjects, as set out in Section 10.
- Assist the Controller in complying with its obligations under Articles 32 to 36 of the UK GDPR, taking into account the nature of the processing and the information available to the Processor.
- Not transfer Personal Data outside the United Kingdom or the European Economic Area except as set out in Section 9.
- Maintain written records of all categories of processing carried out on behalf of the Controller, in accordance with Article 30(2) of the UK GDPR.
- Make available to the Controller the information necessary to demonstrate compliance with Article 28, as set out in Section 14.

6. Confidentiality and Personnel

The Processor shall ensure that access to Personal Data is limited to those personnel who require access in order to perform the Principal Agreement, on a least-privilege and need-to-know basis.

All personnel with access to Personal Data are bound by written confidentiality obligations that survive the end of their engagement, are subject to pre-employment screening in accordance with the Processor's HR Security Policy, and complete security awareness training on appointment and at least annually thereafter.

7. Security

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 the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, in accordance with Article 32 of the UK GDPR.

The measures in force as at the date of this DPA are set out in Annex II. The Processor may update them from time to time provided the level of security is not materially reduced.

8. Sub-Processors

The Controller grants the Processor general written authorisation to engage the Sub-processors listed in Annex III.

The Processor shall engage a Sub-processor only under a written contract imposing data protection obligations materially equivalent to those in this DPA, and shall remain fully liable to the Controller for the performance of that Sub-processor's obligations.

The Processor shall give the Controller at least 30 days' prior written notice of any intended addition or replacement of a Sub-processor. The Controller may object on reasonable data protection grounds within that period. Where an objection cannot be resolved between the parties, the Controller may terminate the affected part of the Principal Agreement without penalty.

The Processor confirms that all Sub-processors providing artificial intelligence capabilities are contractually prohibited from using Controller data, including pupil work and user-generated prompts, to train or improve their own models.

9. International Transfers

All Personal Data held on the Magma Maths platform is hosted within the European Economic Area, in Amazon Web Services region EU-Central-1 (Frankfurt). AI inference takes place within the EU. Transfers from the United Kingdom to the EEA are made in reliance on the UK adequacy regulations.

AI features are enabled by default and may be disabled by the Controller at organisation level at any time. While they are enabled, solution data is sent to the AI sub-processor identified in Annex III for inference within the EU. Solution data consists of the pupil's answer and mathematical working, together with information about the question. Handwritten working is converted into mathematical expressions within the Magma Maths platform before anything is sent, and images of handwriting are not transmitted. Where a pupil uploads a photograph of written work, that photograph is sent so that the work can be read. No pupil names, usernames, email addresses, school names or account identifiers are transmitted. The AI sub-processor does not retain the data or use it for model training. If the Controller disables AI features, no data is sent to the AI sub-processor.

Save as set out above and in Annex III, the Processor shall not transfer Personal Data to a country outside the United Kingdom or the EEA without the Controller's prior written approval. Where such a transfer is approved, the Processor acts as data exporter and shall ensure an appropriate transfer mechanism is in place, being the UK International Data Transfer Agreement, or the EU Standard Contractual Clauses together with the UK Addendum, in each case supported by a transfer risk assessment.

10. Data Subject Rights

Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests to exercise data subject rights under Chapter III of the UK GDPR.

Where the Processor receives a request directly from a data subject in relation to Personal Data processed for the Controller, it shall not respond substantively but shall notify the Controller without undue delay and within five working days.

11. Data Protection Impact Assessments

The Processor shall provide reasonable assistance to the Controller with any data protection impact assessment and any prior consultation with the Information Commissioner's Office relating to the processing. A standard Data Protection Impact Assessment pack for the Magma Maths service is maintained by the Processor and provided to Controllers on request.

12. Personal Data Breach Notification

The Processor shall notify the Controller without undue delay, and in any event within 24 hours, after becoming aware of a Personal Data Breach affecting Personal Data processed for the Controller.

The notification shall, to the extent known at the time and supplemented as further information becomes available, describe:

- The nature of the breach, including the categories and approximate number of data subjects and records concerned.
- The name and contact details of the Processor's data protection contact.
- The likely consequences of the breach.
- The measures taken or proposed to address the breach and mitigate its effects.

The Processor shall cooperate with the Controller and take such reasonable steps as are directed by the Controller to assist in the investigation, mitigation and remediation of the breach, including where the Controller is required to notify the Information Commissioner's Office or affected data subjects.

Where a safeguarding concern about a pupil comes to light, the Processor shall inform the Controller's Designated Safeguarding Lead without delay and in any case the same business day, under its mental health crisis response protocol.

Designated Safeguarding Lead, to be completed by the Controller:

Name	
Email	
Telephone	

13. Government and Law Enforcement Access

If the Processor receives a legally binding request from a public authority for disclosure of Personal Data processed for the Controller, it shall notify the Controller without undue delay unless prohibited from doing so by law. Where prohibited, the Processor shall use reasonable efforts to obtain a waiver of that prohibition and shall

challenge any request it considers unlawful or overbroad. The Processor shall disclose only the minimum amount of Personal Data required.

14. Audit and Inspection

The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 of the UK GDPR, and shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.

In the first instance the Processor shall satisfy such requests by providing its current SOC 2 report, penetration test letter of attestation, policy documentation and completed security questionnaires. Where these do not reasonably satisfy the Controller's audit requirement:

- An audit may be carried out no more than once in any twelve-month period, save where required by a supervisory authority or following a Personal Data Breach.
- The Controller shall give at least 30 days' prior written notice and shall conduct the audit during normal business hours, in a manner that does not unreasonably disrupt the Processor's operations.
- Any auditor mandated by the Controller shall not be a competitor of the Processor and shall be bound by confidentiality obligations.
- Each party shall bear its own costs, save where the audit identifies a material breach of this DPA by the Processor, in which case the Processor shall bear the reasonable costs of the audit.

15. AI Safety and Instructional Standards

While learner-facing artificial intelligence features are enabled, the Processor shall maintain the following standards. AI features are enabled by default and may be disabled entirely by the Controller at organisation level.

The Processor shall avoid anthropomorphising the system. AI-generated content shall be clearly identified and shall avoid the use of first-person language.

The service shall not employ manipulative or persuasive strategies, such as sycophancy, flattery or negative emotional stimulation, to influence pupil behaviour or engagement.

AI output is filtered before it reaches pupils. If content is blocked, the pupil sees an age-appropriate message.

The Processor maintains a documented mental health crisis response protocol governing how concerns about a pupil come to light, escalation to the Controller's Designated Safeguarding Lead, and the handling of related records. This protocol is reviewed at least annually and provided to Controllers on request.

AI features provide formative feedback only. They do not make decisions producing legal or similarly significant effects within the meaning of Article 22 of the UK GDPR, including in relation to pupil grading or attainment.

16. Retention, Return and Deletion

At the Controller's choice, on termination of the Principal Agreement or on written request, the Processor shall return all Personal Data in a structured, commonly used and machine-readable format, delete it, or both. Pupil and class data may also be exported by school administrators at any time in CSV or XLS format.

Retention periods are as follows:

Data	Retention
Pupil data (names, usernames, class, answers and work)	Deleted within 30 days of contract end or account removal
Teacher and administrator accounts	Deleted within 30 days of contract end
Login credentials (hashed)	Deleted within 30 days of contract end
Encrypted backups	Deleted within 30 days of contract end, as backups are overwritten in the standard rotation cycle
Application and access logs	Automatically deleted no later than 90 days after creation
AI interaction data	Automatically deleted no later than 90 days after creation
Temporary processing files	Deleted automatically when processing completes
Support correspondence	Retained for 24 months after last activity, with pupil personal data redacted when the ticket is closed. Deleted within 30 days of contract end or on the Controller's instruction

Personal Data is retained beyond these periods only where required by law, in which case it is kept only for as long as the legal requirement applies and remains subject to the measures in Annex II.

Media sanitisation follows NIST SP 800-88. Written confirmation of deletion is provided to the Controller on request.

17. Records of Processing

The Processor maintains a written record of all categories of processing carried out on behalf of the Controller in accordance with Article 30(2) of the UK GDPR, and shall make it available to the Controller or the Information Commissioner's Office on request.

18. Term and Governing Law

This DPA takes effect on the date of the last signature below and continues for the duration of the Principal Agreement, save for those provisions which by their nature survive termination.

This DPA is governed by the laws of England and Wales and the parties submit to the exclusive jurisdiction of the courts of England and Wales.

19. Signatures

For the Controller	For Radish Education UK Ltd
Organisation:	Radish Education UK Ltd
Name:	Name:
Title:	Title:
Signature:	Signature:
Date:	Date:

Annex I: Description of the Processing

Item	Detail
Controller	To be completed: name and registered address of the school, trust, college, college group or local authority
Processor	Radish Education UK Ltd, 1 Chapel Street, Warwick, CV34 4HL, United Kingdom. Company number 16137150. ICO registration ZB925941.
Subject matter	Provision of the Magma Maths service, an assessment, analytics and personalised learning platform for mathematics
Duration	The term of the Principal Agreement, plus the retention periods set out in Section 16
Nature of the processing	Collection, recording, structuring, storage, retrieval, consultation, automated analysis, transmission within the platform, restriction, erasure and destruction, in each case by automated means within the Magma Maths cloud platform
Purpose of the processing	Authenticating users; presenting and assigning learning content; capturing and storing pupil work; computing class and pupil analytics for educators; generating optional AI-supported formative feedback; maintaining system logs and audit trails for security; supporting the Controller's statutory and contractual functions in education
Categories of data subject	Pupils; teachers; school and trust administrators
Types of Personal Data	Pupils: first and last name, username or school-issued identifier (including email address where provided by school SSO), year group or class, pupil answers and mathematical working (text and drawings), performance analytics. Staff and administrators: name, work email address, school or trust affiliation, feedback given to pupils. System: hashed login credentials, access logs, audit trails.
Special category data	None. No data within the meaning of Article 9 of the UK GDPR is processed.
Criminal offence data	None
Children's data	Yes. The service is used by pupils, including pupils under the age of 13.
Frequency of processing	Continuous for the duration of the Principal Agreement
Automated decision-making	None within the meaning of Article 22 of the UK GDPR
Retention	As set out in Section 16

Annex II: Technical and Organisational Measures

The following measures are in force as at the date of this DPA and are covered by the Processor's SOC 2 Type 1 report (Radish AB, Prescient Assurance LLC, 30 January 2026).

Hosting and infrastructure

- Amazon Web Services, region EU-Central-1 (Frankfurt), deployed across multiple availability zones with automatic failover.
- Separation of development, staging and production environments.
- Multi-tenant architecture with logical segregation enforced by unique tenant identifiers and role-based access control.
- Physical security of data centres is provided by AWS, including 24/7 security, biometric entry controls and video surveillance.

Encryption and cryptography

- Data in transit encrypted using TLS 1.2 or higher.
- Data at rest encrypted using AES-256 with keys managed in AWS KMS.
- Passwords hashed using bcrypt. Digital signatures use RSA-SHA256.
- Endpoint encryption enforced on all company devices (FileVault and BitLocker) and monitored centrally.

Access control

- Role-based access control with least-privilege assignment.
- Multi-factor authentication required for administrative access.
- Single sign-on supported through SAML 2.0 and OpenID Connect.
- Password policy enforcing a minimum length and account lockout after repeated failed attempts.
- Access reviews performed quarterly. Access revoked on termination through a documented offboarding process.

Secure development and vulnerability management

- Secure-by-design and privacy-by-design development standards, with mandatory peer code review before any production merge.
- Source control and CI/CD pipelines with audit trails.
- Annual third-party penetration testing. A letter of attestation is available to Controllers.
- Regular automated vulnerability scanning, with remediation targets of 15 days for critical and high findings, 45 days for medium and 90 days for low.

Monitoring, logging and data loss prevention

- Continuous monitoring of production systems, with alerting to an on-call engineering rota.
- Access and application logging retained for a minimum of 30 days and no more than 90 days.
- Data loss prevention controls implemented.
- Three-tier data classification (confidential, restricted, public) governing handling requirements.

Resilience and business continuity

- Automated encrypted daily backups, automatically rotated.
- Recovery Time Objective of 4 hours and Recovery Point Objective of 15 minutes for the production platform.
- Business continuity and disaster recovery plan tested at least annually.

Organisational measures

- Documented information security management framework, including Information Security, Access Control, Cryptography, Data Management, Operations Security, Secure Development, HR Security, Physical Security, Risk Management, Third-Party Management and Incident Response policies, reviewed at least annually.
- Risk assessment methodology based on ISO 27005, using a five-by-five risk matrix.
- Documented incident response plan with severity classification from P0 (critical) to P3 (low) and defined escalation paths.
- Pre-employment screening, written confidentiality obligations, and security awareness training on appointment and at least annually.
- Third-party and sub-processor risk assessment prior to engagement and on review.

Annex III: Authorised Sub-Processors

Sub-processor	Service	Personal Data received	Location	Transfer mechanism
Amazon Web Services EMEA SARL	Cloud hosting, databases, encrypted storage and backups	All Controller Personal Data, encrypted. AWS has no access to Personal Data in plain form.	Luxembourg, with data hosted in EU-Central-1 (Frankfurt), EEA	Not applicable. Processing within the EEA under the UK adequacy regulations.
Google (optional)	AI model inference for formative feedback. Enabled by default; the Controller may disable AI features at any time	Solution data only: the pupil's answer and working, and information about the question. No names, usernames, email addresses, school names or account identifiers. No retention by the sub-processor and no model training	EU	Not applicable. Processing within the EEA under the UK adequacy regulations.
Wonde Ltd (optional)	MIS integration, where enabled by the school	Roster data only: pupil and staff names, class affiliations, school identifiers	United Kingdom	Not applicable. Processing within the United Kingdom.
Intercom, Inc. (optional)	In-app support chat and ticketing	Name and work email address of staff who contact support, and the content of support conversations. Pupils do not have access	United States	Certified under the UK Extension to the EU-US Data Privacy Framework (UK adequacy regulations). The Controller may opt out of the support chat

The current list of Sub-processors is maintained by the Processor. Changes are notified in accordance with Section 8.

Radish Education UK Ltd, 1 Chapel Street, Warwick, CV34 4HL, United Kingdom. Registered in England and Wales, company number 16137150. ICO registration ZB925941.