

Date of agreement:

DATED

(1) DR FROST LEARNING

School/Trust name:

(2)

DATA PROCESSING AGREEMENT

CONTENTS

	Page
1. Definitions and Interpretation	3
2. Personal data types and processing purposes	5
3. Dr. Frost's obligations	5
4. Dr. Frost employees	5
5. Security	6
6. Personal data breach	6
7. Transfers of personal data	6
8. Subcontractors	6
9. Complaints, data subject requests and third-party rights	7
10. Term and termination	7
11. Data return and destruction	7
12. Records and Audit	7
13. Liability	7
14. Notice	7
APPENDIX A – Personal Data processing purposes and details	9
APPENDIX B – Security measures	10

THIS AGREEMENT is made on 16th March 2026

BETWEEN:-

- (1) **DR. FROST LEARNING** a registered charity in England, with charity number 1194954 whose registered office is at 28 Elmcroft Drive, Chessington, Surrey KT9 1DU (**Dr. Frost**);
- (2) **School/Trust name and address:**

(the Customer).

WHEREAS:-

1. The Customer and Dr. Frost entered into an agreement on or about the academic year 2025/6 (**Services Agreement**). Dr. Frost is providing certain services, the nature of which requires Dr. Frost to process Personal Data on behalf of the Customer.
2. This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which Dr. Frost will process Personal Data when providing services under the Services Agreement. This agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors.

IT IS AGREED as follows:-

1. **DEFINITIONS AND INTERPRETATION**

The following definitions and rules of interpretation apply in this agreement.

1.1 Definitions:

"Business Purposes"	means the services to be provided by Dr. Frost to the Customer as described in the Services Agreement and any other purpose specifically identified in Appendix A.
"Commissioner"	means the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).
"Controller," "Processor," "Data Subject," "Personal Data," "Personal Data Breach" and "Processing"	each have the meanings given in the Data Protection Legislation.
"Data Protection Legislation"	means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party.

"Data Subject"	means the identified or identifiable living individual to whom the Personal Data relates.
"EU GDPR"	means the General Data Protection Regulation ((EU) 2016/679).
"EEA"	means the European Economic Area.
"Personal Data"	means any information relating to an identified or identifiable living individual that is processed by Dr. Frost on behalf of the Customer as a result of, or in connection with, the provision of the services under the Services Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
"Processing, processes, processed, process"	means any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.
"Personal Data Breach"	means a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.
"Records"	has the meaning given in Clause 12.
"Term"	this agreement's term as defined in Clause 10.
"UK GDPR"	has the meaning given in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

- 1.2 This agreement is subject to the terms of the Services Agreement and is incorporated into the Services Agreement. Interpretations and defined terms set forth in the Services Agreement apply to the interpretation of this agreement.
- 1.3 The Annexes form part of this agreement and will have effect as if set out in full in the body of this agreement. Any reference to this agreement includes the Annexes.
- 1.4 A reference to writing or written excludes fax but not email.
- 1.5 In the case of conflict or ambiguity between:
 - 1.5.1 any provision contained in the body of this agreement and any provision contained in the Annexes, the provision in the body of this agreement will prevail;

- 1.5.2 the terms of any accompanying invoice or other documents annexed to this agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and
- 1.5.3 any of the provisions of this agreement and the provisions of the Services Agreement, the provisions of this agreement will prevail.
- 1.6 References in this Agreement to any statute, statutory provision or subordinate legislation include a reference to that statute, statutory provision or subordinate legislation as amended, extended, consolidated, re-enacted or replaced from time to time, and to any subordinate legislation made under it

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

- 2.1 The Customer and Dr. Frost agree and acknowledge that for the purpose of the Data Protection Legislation:
 - 2.1.1 the Processor is Dr. Frost and the Customer is the Controller.
 - 2.1.2 the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to Dr. Frost.
 - 2.1.3 Appendix A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which Dr. Frost may process the Personal Data to fulfil the Business Purposes.

3. DR. FROST'S OBLIGATIONS

- 3.1 Dr. Frost will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. Dr. Frost will not process the Personal Data for any other purpose or in a way that does not comply with this agreement or the Data Protection Legislation. Dr. Frost must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.
- 3.2 Dr. Frost must comply promptly with any Customer written instructions requiring Dr. Frost to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 3.3 Dr. Frost will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Customer or this agreement specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Commissioner). If a domestic or EU law, court or regulator (including the Commissioner) requires Dr. Frost to process or disclose the Personal Data to a third-party, Dr. Frost must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.
- 3.4 Dr. Frost will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of Dr. Frost's processing and the information available to Dr. Frost, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.
- 3.5 Dr. Frost must notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting Dr. Frost's performance of the Services Agreement or this agreement.

4. DR. FROST EMPLOYEES

- 4.1 Dr. Frost will ensure that all of its employees:
 - 4.1.1 are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

- 4.1.2 have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and
- 4.1.3 are aware both of Dr. Frost's duties and their personal duties and obligations under the Data Protection Legislation and this agreement.

5. SECURITY

- 5.1 Dr. Frost must at all times implement appropriate technical and organisational measures against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Appendix B.
- 5.2 In determining the measures to be maintained pursuant to Clause 5.1 above, Dr. Frost shall:
 - 5.2.1 consider whether the pseudonymisation and encryption of personal data is appropriate;
 - 5.2.2 take into account the need to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 5.2.3 take into account the need the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
 - 5.2.4 where appropriate, have in place a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. PERSONAL DATA BREACH

- 6.1 Dr. Frost will notify the Customer in writing without undue delay if it becomes aware of:
 - 6.1.1 the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data;
 - 6.1.2 any accidental, unauthorised or unlawful processing of the Personal Data; or
 - 6.1.3 any Personal Data Breach.
- 6.2 On reasonable suspicion of any of the above, Dr. Frost shall conduct an initial assessment to determine, with a reasonable degree of certainty, whether the event or incident qualifies for notification to the Customer and shall provide a copy of this initial assessment along with such notification.

7. TRANSFERS OF PERSONAL DATA

Dr. Frost (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK or, the EEA without obtaining the Customer's prior written consent.

8. SUBCONTRACTORS

- 8.1 Dr. Frost may authorise a third-party (subcontractor) to process the Personal Data if:
 - 8.1.1 the Customer provides written consent prior to the appointment of each subcontractor, which shall include the list of subcontractors set out in Appendix A; and
 - 8.1.2 Dr. Frost enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of the relevant excerpts from such contracts.
- 8.2 Where the subcontractor fails to fulfil its obligations under the written agreement with Dr. Frost which contains terms substantially the same as those set out in this agreement, Dr. Frost remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

9. **COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD-PARTY RIGHTS**

9.1 Dr. Frost must, at the Customer's expense, assist the Customer in responding to any request from a Data Subject and in ensuring compliance with the Customer's obligations under applicable Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with the Commissioner, supervisory authorities and other regulators and, in particular, Dr. Frost shall promptly notify the Customer if it receives any complaint, notice or communication (whether from the Commissioner, any Data Subject, supervisory authority or other third party, which relates to the processing of the Customer Personal Data).

10. **TERM AND TERMINATION**

10.1 This agreement will remain in full force and effect so long as:

10.1.1 the Services Agreement remains in effect; or

10.1.2 Dr. Frost retains any of the Personal Data related to the Services Agreement in its possession or control (**Term**).

10.2 Any provision of this agreement that expressly or by implication should come into or continue in force on or after termination of the Services Agreement in order to protect the Personal Data will remain in full force and effect.

11. **DATA RETURN AND DESTRUCTION**

11.1 At the written direction of the Customer, Dr. Frost shall delete or return to the Customer all Personal Data in its possession on termination or expiry of this agreement, unless Dr. Frost is required by applicable law to continue to process that Personal Data, in which case Dr. Frost will notify the Customer, in writing, of the applicable law and shall only be permitted to process such Personal Data for the specific purpose so-notified. All other requirements set out in this Agreement shall continue to apply to that Personal Data for so long as it is processed by Dr. Frost.

12. **RECORDS AND AUDIT**

12.1 At least once a year, Dr. Frost will conduct site audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

12.2 On the Customer's written request, Dr. Frost will make all of the relevant audit reports available to the Customer for review. The Customer will treat such audit reports as Dr. Frost's confidential information under the Services Agreement.

13. **LIABILITY**

13.1 Any limitation of liability set forth in the Services Agreement will apply to this agreement.

14. **NOTICE**

14.1 Any notice given to a party under or in connection with this agreement shall be in writing and shall be:

14.1.1 delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case) and

14.1.2 sent by email to the following addresses (or an address substituted in writing by the party to be served):

Data privacy contact email

(a) For the Customer:

(b) For Dr. Frost: support@drfrost.org

14.2 Any notice shall be deemed to have been received:

14.2.1 if delivered by hand, at the time the notice is left at the proper address; or

14.2.2 if sent by next working day delivery service, at 9:00am on the second Business Day after posting; or

14.2.3 if sent by email, at the time of transmission, or, if this time falls outside Business Hours in the place of receipt, when Business Hours resume.

14.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This agreement has been entered into on the date stated at the beginning of it.

Name and position of signatory

Signed by

for and on behalf of

Signed by Katharine Jackson CEO

A handwritten signature in black ink, appearing to read 'K Jackson', written in a cursive style.

for and on behalf of Dr Frost Learning

APPENDIX A – PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Subject matter of processing: processing pupil and instructor data for purposes of accessing online academic materials and services, including but not limited to the following:

- Usability of the platform
- Account administration and sign-up
- Customer support
- Maintaining security of the platform and personal data
- Informing pupils and instructors about the functionality of the platform (including by way of newsletter)
- Circulating tips for navigation and effective use of the platform
- Enabling instructors to invite colleagues and students to sign-up and use the service

Duration of Processing: Co-terminus with the Services Agreement

Nature of Processing: As set out in the Services Agreement

Business Purposes: processing on the instructions of the Customer and to ensure the Customer, its instructors and students can receive and access the services

Personal Data Categories: Student first and last names, student email addresses, grade and school of student

Data Subject Types: Students

Approved Subcontractors:

- Google Cloud - hosting
- Sentry - monitoring
- CloudFlare - CDN and security
- Zendesk - support
- PostHog - analytics
- Slack - for support messages

APPENDIX B – SECURITY MEASURES

1) Data in transit protection

- The Platform uses a minimum of TLS 1.2 used for all site traffic between user device and Platform endpoints.
- Data in transit internally to Dr Frost systems can only travel via Virtual Private Cloud (VPC) which is not accessible externally except by a small number of admin users over SSL tunnel.

2) Asset protection and resilience

- Data are physically located in a Google Cloud secured data centre in the UK.
- Dr Frost does not use any PII for marketing purposes, machine learning, AI or any purpose other than providing The Services. The Platform database uses encrypted at rest data storage.
- Dr Frost does not store user data on any other physical medium and user data never leaves the Google Cloud data centre except for transmission in the provision of The Services.

3) Separation between customers

Dr Frost is not able to provide physical separation of user data or compute. Information about other users in a given school or trust organisation is only available to other users in that organisation. This separation is provided in software only and not at a physical or hardware level.

4) Operational security

Dr Frost will take all reasonable measures to address any vulnerabilities within a reasonable period of time. To that end, we use an automated build process to maintain up-to-date patch levels on the Virtual Machines that host The Platform.

5) Personnel security

- Dr Frost limits access to user data to a small number of support and development staff. All staff are required to have multi-factor authentication enabled on their administrative accounts.
- All Dr Frost employees are subjected to DBS checks.

6) Secure development

- Dr Frost is continually improving its development workflow and uses an automated release process to provide an auditable trail of software released through development and production environments.
- All configuration is managed in source control or Google Cloud Platform Secrets Manager wherever appropriate.

7) Supply chain security

No customer data is made available to third parties for any commercial purpose ever. We may, however, occasionally share limited anonymised data with for the express purpose of assessing Dr Frost's impact on improving educational outcomes.

8) Secure user management, identity and authentication

Dr Frost offers authentication via Google and Microsoft O365 SSO and strongly recommends that users utilise this wherever possible.

9) External interface protection

- The only external interfaces available to access Dr Frost systems are the Google Cloud service console and direct database access over SSL tunnel to a specific bastion server.
- Both are only accessible by a small number of Dr Frost employees and use Google Cloud RBAC to limit permissions only to what is needed for each individual. Multi-factor authentication is enforced on all Dr Frost Google Workspace accounts.

10) Secure service administration and auditing

The Platform records actions taken by school staff, such as user deletion, class data imports, changes to class membership and so on. This audit data can be viewed by any teacher at that school on the Audit Log accessible from the Classes page.