*Dr Frost Learning Data Processing Agreement - Version 2.0*

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services between:

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** which is a company registered in England and Wales under company number \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and whose registered office is at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “**Company**”)

and

***Dr Frost Learning*** whose address is *c/o Tiffin School, Queen Elizabeth Road, Kingston upon Thames, KT2 6RL* (the “**Processor**”)

(together as the “**Parties**”)

**WHEREAS**

(A) The Company acts as a Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Processor.

(C) The Parties seek to implement an Agreement that complies with the requirements of the current legal framework in relation to data processing, in particular The General Data Protection Regulation of the UK on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and the UK Data Protection Act 2018, as amended from time to time.

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

**1. Definitions and Interpretation**

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.1.2 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "**Contracted Processor**" means a Subprocessor;

1.1.4 "**Data Protection Laws**" means GDPR and the Data Protection Act 2018, as amended from time to time;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**GDPR**" means UK General Data Protection Regulation as amended from time to time;

1.1.7 "**Data Transfer**" means:

1.1.7.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.7.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.8 "**Services**" means the processing that the Processor is authorised to do on behalf of the Company as listed in Schedule 1 (Authorised Processing Template).

1.1.9 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

**2. Processing of Company Personal Data**

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company’s documented instructions.

2.2 The Company instructs Processor to process Company Personal Data related to its DrFrostMaths software.

**3. Processor Personnel**

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor and any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

**4. Security**

4.1 Processor is obligated to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed, 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 risks of varying likelihood and severity for the rights and freedoms of natural persons, including inter alia as appropriate:

a) the pseudonymisation and encryption of Personal Data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c)  the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

4.2 The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to the Personal Data does not Process the Personal Data except on instructions of the Company, unless he or she is required to do so under Data Protection Law.

4.3 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

**5. Subprocessing**

5.1 Processor shall not appoint, replace or disclose any Company Personal Data to any Subprocessor unless required or authorised by the Company.

5.2 The Processor agrees to enter into a written agreement with each Subprocessor it engages, which imposes the same obligations on the Subprocessors as are imposed on the Processor under this Agreement. The Controller will, at any time upon reasonable prior written notice, be entitled to receive a copy of the Processor’s data processing agreement with each Subprocessor.

5.3 The Company will not prevent the Processor from engaging any existing Subprocessor, without a bona fide and objective reason.

5.4 Where a Subprocessor fails to fulfil its data protection obligations under the Data Processing Agreement referred to in clause 7.1 (Personal Data Breach), the Processor shall remain fully liable to the Controller for the performance of the Sub-processor’s fulfilment of its data protection obligations in general.

5.5 The Processor agrees to give the school the opportunity to object to any changes to the Subprocessors used by the Processor.

**6. Data Subject Rights**

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data or a complaint; and

6.2.2 ensure that it does not respond to that request or complaint except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request;

6.2.3 promptly notify Company if it receives any communication from a Supervisory Authority (e.g. the UK Information Commissioners Office) or any other regulatory authority in connection with Personal Data processed under this Agreement;

6.2.4 promptly notify Company if it receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law.

**7. Personal Data Breach**

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report the Personal Data Breach to the UK Information Commissioners Office and / or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

**8. Data Protection Impact Assessment and Prior Consultation**

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

Such assistance may include:

* + 1. a systematic description of the envisaged processing operations and the purpose of the processing;
    2. an assessment of the necessity and proportionality of the processing operations in relation to the Services;
    3. an assessment of the risks to the rights and freedoms of Data Subjects; and
    4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

**9. Deletion or return of Company Personal Data**

9.1 Subject to this section 9, Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within 10 business days of the Cessation Date.

**10. Audit rights**

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 For the purpose of auditing the Processor’s compliance with its obligations under this Agreement, the Processor shall allow for the Company, on reasonable written notice of not less than 10 days, to perform an Audit, including but not limited to:

a) gain access to inspect, and take copies of, the records and any other information held at the Processor’s premises or on the Processor System related to the Data Processing Services, and;

b) gain access to inspect the Processor System.

10.3 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law. For the avoidance of doubt, the Company is not allowed to disclose to the public any parts of the audit report, without prior written consent from the Processor, unless required by mandatory law.

**11. Data Transfer**

11.1 The Processor may not transfer or authorise the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data, which ensure Data Subjects have enforceable rights and effective legal remedies.

**12. General Terms**

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

**13. Governing Law and Jurisdiction**

13.1 This Agreement is governed by the laws of England and Wales.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of England.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

**The Company**

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**The Processor**

Signature \_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_Dr Jamie Frost\_\_\_\_\_\_\_\_\_

Title \_\_\_\_\_\_CEO\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date Signed \_\_\_\_\_30/11/22\_\_\_\_\_\_\_\_\_

**Schedule 1 - Authorised Processing Template**

* + 1. The contact details of the Company Data Protection Officer are:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Phone – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. The contact details of the Supplier Data Protection Officer are:

Dr Jamie Frost, c/o Tiffin School, Queen Elizabeth Road, Kingston upon Thames, KT2 6RL

Email - [jamie@drfrostmaths.com](mailto:jamie@drfrostmaths.com)

* + 1. The Processor shall comply with any further written instructions with respect to processing by the Controller.
    2. Any such further instructions shall be incorporated into this Schedule.

|  |  |
| --- | --- |
| Identity of the Controller and Processor | The Parties acknowledge and agree that for the purposes of the Data Protection Legislation, the Controller and Processor are as set out in this Data Processing Agreement. |
| Nature and purposes of the processing | Dr Frost Learning allows teachers to set and monitor homework assignments, in which students log in and complete assigned questions.  Students may also decide to initiate independent practices themselves, again where their linked teacher accounts can monitor this data.  There are a variety of other tools, e.g. the ability for teachers to create printed worksheets/assessments, and a networked 'virtual whiteboard' in which teacher and student whiteboards are connected.  Teachers set up student accounts, with the name and email address of the student provided by the teacher or student, the latter data purely for the purposely of allowing easier login, automated password resetting and email notifications of new homework set by a teacher. The DFM system stores performance data of the student to enable both the teacher and data to make assessments of progress. |
| Type of Personal Data | * Title *(Teachers only)* * Name * School Email address * School Attended Name * Year Group * Parental consent indicator (to register student) * Assessment tasks completed * Performance data against assigned tasks/homework * Teacher / student feedback |
| Categories of Data Subject | Students  Staff |
| Retention Period | Personal data will be retained in the line with Companies Records Retention Policy for such records.  Dr Frost Learning will automatically purge inactive accounts where the user has not logged in over 2 years. It is the school's responsibility to delete the accounts of students who have left the school (via the Manage Classes interface) if they wish to delete accounts before this time. |