MOSSPAM
SYSTEMATICALLY OPTIMISING SCHOOL PERFORMANCE

DATA PROCESSOR AGREEMENT

23 MAY 2018

AGREEMENT OF SHARING OF DATA

BETWEEN

MOSSPAM

AND

[School]

MOSSPAM
SYSTEMATICALLY OPTIMISING SCHOOL PERFORMANCE

This agreement (the "Agreement") is made

Introduction

This agreement regarding processing of personal data (the "Data Processor Agreement") regulates MossPAM's (the "Data Processor") processing of personal data on behalf of the school (the "Data Controller") and is attached as appendix A to the MossPAM Software as a Service Agreement (the "Main Agreement"), in which the parties have agreed the terms for the Data Processor's delivery of services to the Data Controller (the "Main Services").

Parties

1. MossPAM, 100 Downs Park Road E5 8JY, Company registration no. 10248621,
"The Data Processor"

2. [SCHOOL]
"The Data Controller"

Each referred to as a "Party" and together the "Parties".

1. Legislation

1.1 The Data Processor Agreement shall ensure that the Data Processor complies with the applicable data protection and privacy legislation (the "Applicable Law"), including in particular:

(i) The European Parliament and the Council's Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data that entered into force on 24 May 2016 and will be applicable on 25 May 2018 ("GDPR").

2. Processing of personal data

2.1 In connection with the Data Processor's delivery of the Main Services to the Data Controller, the Data Processor will process certain categories and types of the Data Controller's personal data on behalf of the Data Controller.

2.2 "Personal data" include "any information relating to an identified or identifiable natural person" as defined in GDPR, article 4 (1) (1) (the "Personal Data"). The categories and types of Personal Data processed by the Data Processor on behalf of the Data Controller are listed in sub-appendix A. The Data Processor only performs processing activities that are necessary and relevant for MossPAM to perform the Main Services. The parties shall update sub-appendix A whenever changes occur that necessitates an update.

2.3 The Data Processor shall have and maintain a register of processing activities in accordance with GDPR, article 32 (2). The processing activity of The Data Processor will be visible to the Data Controller via the Main Service.

3. The data Processor's obligations

3.1 Confidentiality

3.1.1 The Data Processor shall treat all the Personal Data as strictly confidential information. The Personal Data shall only be copied, transferred or otherwise processed in accordance with The Applicable Law and with the written permission of The Data Controller.

3.1.2 The Data Processor's employees shall be subject to an obligation of confidentiality that ensures that the employees shall treat all the Personal Data under this Data Processor Agreement with strict confidentiality.

3.2 Security

3.2.1 The Data Processor shall ensure that access to the Personal Data is restricted to only the employees of MossPAM and P4IT Kft. to whom it is necessary and relevant to process the Personal Data in order for the Data Processor to perform its obligations under the Main Agreement and this Data Processor Agreement.

3.2.2 The Personal Data is SSL transferred from the Data Controller to a secure server farm located in the EEA, see sub-Appendix C. The Personal Data is accessed from the Data Controller via an SSL certificate.

3.2.3 Once Personal Data is destroyed from the Data Controller's MIS, The Data Processor will anonymise this data in The Main Service within seven days.

3.3 Data protection impact assessments and prior consultation

3.3.1 If the Data Processor's assistance is necessary and relevant, the Data Processor shall assist the Data Controller in preparing data protection impact assessments in accordance with GDPR, article 35, along with any prior consultation in accordance with GDPR, article 36.

3.3.2 The Data Processor will complete impact assessments twice a year in accordance with GDPR.

3.4 Rights of the data subjects (Subject Access Requests)

3.4.1 If the Data Controller receives a request from a data subject for the exercise of the data subject's rights under the Applicable Law and the correct and legitimate reply to such a request necessitates the Data Processor's assistance, the Data Processor shall assist the Data Controller by providing the necessary information and documentation. The Data Processor shall be given reasonable time to assist the Data Controller with such requests in accordance with the Applicable Law.

3.4.2 If the Data Processor receives a request from a data subject for the exercise of the data subject's rights under the Applicable Law and such request is related to the Personal Data of the Data Controller, the Data Processor must immediately forward the request to the Data Controller and must refrain from responding to the person directly.

3.5 Personal Data Breaches

3.5.1 The Data Processor shall give immediate notice to the Data Controller if a breach of the data security occurs, that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, personal data transmitted, stored or other wise processed re the Personal Data processed on behalf of the Data Controller (a "Personal Data Breach").

3.5.2 The Data Processor shall have and maintain a register of all Personal Data Breaches. The register shall at a minimum include the following:

(i) A description of the nature of the Personal Data Breach, including, if possible, the categories and the approximate number of affected Data Subjects and the categories and the approximate number of affected registrations of personal data.

(ii) A description of the likely as well as actually occurred consequences of the Personal Data Breach.

(iii) A description of the measures that the Data Processor has taken or proposes to take to address the Personal Data Breach, including, where appropriate, measures taken to mitigate its adverse effects.

3.5.3 The register of Personal Data Breaches shall be provided to the Data Controller in copy if so requested in writing by the Data Controller or the relevant Data Protection Agency.

3.6 Documentation of compliance

3.6.1 The Data Processor shall after the Data Controller's written request hereof provide documentation substantiating that:

(i) the Data Processor complies with its obligations under this Data Processor Agreement;

(ii) the Data Processor complies with the Applicable Law in respect of the processing of the Data Controller's Personal Data.

3.6.2 The Data Processor's documentation of compliance shall be provided within reasonable time.

3.7 Location of The Personal Data

3.7.1 The Personal Data is processed by the Data Processor and approved sub-processors as per Section 4. The data is not transferred outside of the EEA. The data is stored securely in servers based in the EEA. See sub-Appendix C for Server details

3.7.2 Any transfer of the Personal Data to any new third countries or international organisations in the future shall only be done to the extent such transfer is permitted in writing from The Data Controller and done in accordance with the Applicable Law.

3.8 Vulnerability Scanning & Testing

3.8.1 The Data Processor will conduct vulnerability scanning and testing of The Main Service in accordance with GDPR, article 32.

3.8.2 Visibility of IT system online tests will be conducted quarterly.

3.8.3 Firewall security testing

3.8.4 PHP related configuration files are scanned regularly, existence of security settings regularly examined.

4. Sub-Processors

4.1 The Data Processor authorises the Sub-Processor to process the Personal Data as per the Data Processor Agreement.

4.2 The Data Processor is accountable to the Data Controller for any Sub-Processor in the same way as for its own actions and omissions.

4.3 The Data Processor is at the time of entering into this Data Processor Agreement using the Sub Processors listed in sub-appendix B. The Data Processor will only initiate sub-processing with a new Sub-Processor after notifying and receiving written confirmation from The Data Controller. The new Sub-Processor will be added to the list in sub-appendix B.

5. Security and Training

5.1 The Parties agree to implement appropriate technical and organisational measures to protect the Shared Personal Data in their possession against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, including but not limited to:

- Ensuring IT equipment, including portable equipment is kept in lockable areas when unattended;
- not leaving portable equipment containing the Personal Data unattended;
- ensuring that staff use appropriate secure passwords for logging into systems or databases containing the Personal Data;
- ensuring that all IT equipment is protected by antivirus software, firewalls, pass words and suitable encryption devices;
- limiting access to relevant databases and systems to those of its officers, staff agents and sub-contractors who need to have access to the Personal Data, and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged by the Party;
- Ensuring all staff handling Personal Data have been made aware of their responsibilities with regards to handling of Personal Data.

- Staff accessing The Main Service outside of their respective Data Controller's IP range will be prompted to double-factor authenticate their account.
- Staff accessing the Main Service within their respective Data Controller's IP Range will be prompted to provide authentication (via Password and username).
- Conducting regular threat assessment or penetration testing on systems.

6. Duration

6.1 The Data processor Agreement shall remain in force until the Main Agreement is terminated

7. Termination

7.1 The Data Processor's authorisation to process Personal Data on behalf of the Data Controller shall be annulled at the termination of this Data Processor Agreement.

7.2 The Data Processor shall continue to process the Personal Data for up to three months after the termination of the Data Processor Agreement to the extent it is necessary and required under the Applicable Law. In the same period, the Data Processor is entitled to include the Personal Data in the Data Processor's backup. The Data Processor's processing of the Data Controller's Personal Data in the three months after the termination of this Data Processor Agreement shall be considered as being in accordance with the Instruction.

7.3 At the termination of this Data Processor Agreement, the Data Processor and its Sub Processors shall return the Personal Data processed under this Data Processor Agreement to the Data Controller, provided that the Data Controller is not already in possession of the Personal Data. The Data Processor is hereafter obliged to delete all the Personal Data and provide documentation for such deletion to the Data Controller.

8. Roles and Responsibilities

8.1 Each Party shall nominate a single point of contact within their organisation who can be contacted in respect of queries or complaints regarding the DPA, GDPR and/or compliance under the terms of this Agreement.

MOSSPAM	SCHOOL
Data Protection Officer MossPAM 100 Downs Park Road London E5 8JY enquiries@mosspam.org +44 (0) 208 525 5210	

9. Variation

9.1 No variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

10. Warranties

10.1 Each Party warrants and undertakes that it will:

(a) Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its personal data processing operations.

(b) Make available upon request to the Data Subjects who are third party beneficiaries a copy of this agreement unless the Clause contains confidential information.

(c) Respond within a reasonable time and as far as reasonably possible to enquiries from the relevant Data Protection Authority in relation to the Shared Personal Data.

(d) Respond to Subject Access Requests in accordance with the terms of this Agreement and in accordance with the DPA.

(e) Where applicable, maintain registration with all relevant Data Protection Authorities to process all Shared Personal Data for the Agreed Purpose

Signed for and on behalf of MossPAM

Name: [CEO, COO]

Signature:

Signed for and on behalf of [School]

Name:

Position:

Signature:

Sub-Appendix A

1. Personal Data

1.1 The Data Processor processes the following types of Personal Data in connection with its delivery of the Main Services from the Data Controllers MIS:

(i) Personal data provided by the users in connection with their use of the Main Services (these personal data are not seen or accessed by the Data Processor unless the Data Processor after the request hereof from the Data Controller assists with support and bug fixing).

1.2 Student Data held on The Service (via MIS & Directly Inputted):

Forename & Legal Forename
Surname & Legal Surname
Middle Name
Date of birth
Gender
SEN Status Code, Name & Date
Ethnicity Code & Name
Religion
First Language Code & Name
Year Group
Admission Number & Date
Leaving Date
FSM
Pupil Premium
EAL
Exam Number
Reg Group Name
Progress & Attainment Data
Parent/Carers Details (Addresses, Contact Numbers, Relationship to child, Email Address)
Parent/Carers Letter Sent to and Reply Slips
Student Strategies & Behaviour
Photograph
Subjects Studied & Timetable
Public Examination Data

1.3 **Staff Data held on The Main Service (via MIS & Directly Inputted):**

Title
Forename & Legal Forename
Surname & Legal Surname
Middle Name
Gender
Date Leaving
Employment Date Start
Performance Management
Lesson Observations
Management Role(s)
Timetable & Subjects Taught
Work Email
Teacher Code
System Access Log
Photograph

Sub-Appendix B

1. Approved Sub-Processors

1. 1 The following Sub-Processors shall be considered approved by the data Controller at the time of entering into this Data Processor Agreement:

(i) P4IT Kft.

2. New Sub-Processors

2.1 The following Sub-Processors have been added and communicated to the Data Controller prior to the relevant sub-processing:

(i) [Insert When Relevant]

Sub-Appendix C

1. Server Details

1.1 Full root access dedicated IPv4 Address, with a rescue system and twenty-four (24) hour server monitoring.

1.2 Located within the EEA

1.3 Dedicated twenty-four (24) hour stand-by-service with CCTV monitoring.