

1. Introduction

- 1.1 This Data Processing Agreement has been agreed between the following parties:
- Data Controller: **[School Name]**
- And
- Data Processor: **School Synergy Limited**
- 1.2 This Agreement details the specific purpose(s), including legislative powers and duties, for passing personal data between the Data Controller and the Data Processor or accessed by the Processor on the Controller's authority.
- 1.3 It will indicate the degree of confidence that each party has in respect of their ability to fulfil the commitments outlined in the GDPR, if any issues need to be addressed, who they are incumbent upon, the timeframe for completion and how they will be measured and reviewed.
- 1.4 This Agreement is binding on both parties and each organisation will work towards meeting the commitments made. It is a working document and therefore the contents can be reviewed and altered at any time to reflect the changing circumstances. Such changes would be subject to the agreement of both parties.
- 1.5 This Agreement is accompanied by the Processor's Data Protection Policy and Data Breach Policy.

2. Definitions

- 2.1 **Service:** School Synergy Service.
- 2.2 **Data:** All personal data collected, generated or otherwise processed by the Processor as a result of, or in connection with, the provision of the Service.
- 2.3 **Data Protection Laws:**
- (a) General Data Protection Regulation (EU 2016/679) (GDPR) and any legislation which amends, re-enacts or replaces it in England and Wales.
 - (b) Electronic Communications (EC Directive) Regulations 2003, together with any legislation which replaces it.
 - (c) The UK's third generation of data protection (Data Protection Act 2018).
- 2.4 **Data Subject:** An individual who is the subject of personal data.
- 2.5 **Supervisory Authorities:** Any Data Protection authority with jurisdiction over the processing of data.

3. Data Processing

- 3.1 The Processor will comply with the requirements of the Data Protection Laws in respect of the activities which are the subject of the Agreement and shall not knowingly do anything or permit anything to be done which may lead to a Data Breach or breach of the Data Protection Laws.

- 3.2 The Processor will only process Data to the extent it relates to the nature and purpose and the categories of Data Subject as set out in the Schedule and only for the duration of the contract.
- 3.3 The Processor will
- (a) Only process the data in accordance with solution and service provided and on agreement with the Controller.
 - (b) Inform the Controller if it believes that the Controller's instructions infringe the Data Protection Laws.
 - (c) Have in place and maintain throughout the terms at all times in accordance with the then current good industry practice, all appropriate technical and organisational security measures against unauthorised or unlawful processing, use, access to or theft of the data including loss or destruction or damage to the data.
 - (d) Ensure that all persons authorised by the Processor to process data are bound by obligations and contracts.
 - (e) Ensure that data is limited to those personnel who need to access the data as part of the processing duties and to log all requests by the Controller for the Processor to view data when requested for support purposes.
- 3.4 The Processor will provide the controller with assistance in response to specific Data Subject access requests in order for the Controller to meet their obligations.
- 3.5 The Processor will assist the Controller with appropriate audits, inspections and other information needed to ensure that both the Controller and the Processor are meeting their Article 28 obligations from the GDPR Data Protection Laws. Requests beyond standard requests such as data or security forensics beyond the expected level may incur a charge to cover this cost.

4. Transfers Outside of the EU

- 4.1 The Processor will not process or transfer any data outside of the EU for processing.

5. Sub-Processors

- 5.1 The Processor will not engage any third party to carry out processing in connection with the Service except that of standard operating practices such as transit communication for sending email through services such as Microsoft and text carriers such as Vodafone without consent from the Controller.

6. Supervisory Authorities

- 6.1 The Processor will promptly provide assistance and information which is requested by any Supervisory Authority as per required under legal obligations.
- 6.2 The Processor will notify the controller of any such request unless prohibited by law.

7. Records

- 7.1 The Processor will maintain records of all processing activities carried out on behalf of the Data Controller including:

- (a) the name of the Data Protection Officer
- (b) the different types of processing being carried out
- (c) a description of the technical and organisational security measures in place

8. Data Subjects

- 8.1 On request the Processor will assist where the Controller is unable to complete tasks to comply with their obligations under the Data Protection Laws in relation to:
- (a) the provision of information to Data Subjects
 - (b) the rectification of inaccurate Data in relation to a Data Subject
 - (c) the erasure of a Data Subject's Data

9. Data Breaches

- 9.1 This Agreement incorporates the accompanied Data Breach Policy.
- 9.1 The Processor will comply with the requirements of the Data Protection Laws in respect of the activities which are subject to the Agreement and will not knowingly do anything or permit anything to be done which might lead to a breach by the Controller of the Data Protection Laws.
- 9.2 The Processor will immediately inform the Controller if it believes that the Controller infringes the Data Protection Laws.
- 9.3 The Processor will immediately inform the Controller of any Data Breach of that of the Processor as per the steps in the accompanied Data Breach Policy.
- 9.4 The Processor will make any appropriate notifications to the Supervisory Authorities where legally required to do so.

10. Return of Destruction of Data

- 10.1 The Processor will destroy and/or return all Data to the Controller on termination of this Agreement and shall delete all copies it holds of the Data unless relevant laws require the Processor to retain.

11. Warranties


- 11.1 The Processor warrants that
- (a) It will process the Data in compliance with all applicable laws, regulations, orders and standard including the Data Protection Laws.
 - (b) It will take appropriate technical and organisational measures against the unauthorised or unlawful processing of Data and against the accidental loss or destruction or damage to Data to ensure the Controller's compliance with the Data Protection Laws.
 - (c) The Processor will notify the Controller immediately if it becomes aware of any unauthorised or unlawful processing, loss, damage or destruction of the data.
- 11.2 The Controller warrants that

- (a) It will provide the Processor with all Data in compliance with all applicable laws, regulations, orders and standard including the Data Protection Laws.
- (b) The Data supplied has been obtained fairly and lawfully.
- (c) It obtains all necessary consents from persons whose Data is being processed and registrations with authorities to permit the transfer of Personal Data to the Processor.
- (f) The Controller maintains in accordance with the then current good industry practice, all appropriate technical and organisational security measures on using the data as provided by the Service.

12. Data Categories

- 12.1 Personal Data from the Controllers Management Information System is processed by the Processor. This is transparent within the Service and includes information such as identifiable student, staff and parent information. The Processor aims to only process the minimum fields for the Controller to perform their functions whilst using the Service.
- 12.2 The list of fields will vary throughout the Agreement in part due to the Controller selecting their own user defined fields to be processed. The Processor makes the data transfer transparent. Authorised members of the Controller's Data Protection team or Administrator can inspect and audit these directly through the Service.
- 12.3 Data such as IP address, log-in data and cookies will be logged for purposes of security and auditing in order for the Processor to maintain expected security measures These will be periodically deleted once those functions have been completed.

Signed on behalf of the Processor (School Synergy Limited)

Authorised Name	Alan Cree
Position	Managing Director
Date	15/05/2019
Signature	

Signed on behalf of the Controller (School Name)

Authorised Name	
Position	
Date	
Signature	