DATA PROCESSOR ADDENDUM

1. DEFINITIONS

1.1 The terms **"process/processing", "data subject", "processor", "controller", "personal data", "personal data breach"**, and **"data protection impact assessment"** shall have the same meaning ascribed to them in Data Protection Laws;

1.2 "**Addendum**" means this Data Processor Addendum;

1.3 **"Customer"** means the Customer or Licensee under the Main Agreement;

1.4 **"Data Protection Laws" means, in relation to any Protected Data:**

(a) the UK General Data Protection Regulation (UK GDPR), being the version of Regulation (EU) 2016/679 retained in UK law following the European Union (Withdrawal) Act 2018;

(b) the Data Protection Act 2018;

(c) any other applicable UK law relating to the processing, privacy and/or use of personal data; and

(d) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing.

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

1.6 "**Main Agreement**" means the license or services agreement into which this Addendum is incorporated;

1.7 "**Protected Data**" means the data described in Annex 1 (*Details of Processing of Personal Data*) and any other personal data processed by the Supplier (or a Sub-processor) on behalf of the Customer pursuant to or in connection with the Main Agreement;

1.8 "**Services**" means the services described in the Main Agreement;

1.9 "Standard Contractual Clauses" means for transfers of personal data from the UK, the International Data Transfer Agreement (IDTA) or the UK Addendum to the European Commission's 2021 Standard Contractual Clauses, or any successor clauses formally approved by the UK Information Commissioner's Office (ICO); and for transfers of personal data from the EEA (where relevant), the European Commission's standard contractual clauses adopted in Implementing Decision (EU) 2021/914, or any amendments or replacements.

1.10 "**Sub-processor**" means any processor (including any affiliate of the Supplier) appointed by the Supplier (or by any Sub-processor) to process Protected Data on behalf of the Customer;

1.11 "Supervisory Authority" means a regulatory authority responsible for overseeing compliance with applicable Data Protection Laws, including the UK Information Commissioner's Office (ICO), and any equivalent authority in a relevant jurisdiction.

1.12 **"Supplier"** means the Supplier or Licensor under the Main Agreement.

2. PROCESSING OF PROTECTED DATA

2.1 The parties agree that the Customer is the controller and that the Supplier is the processor for the purposes of processing Protected Data.

2.2 Each party shall at all times in relation to the processing of Protected Data comply with Data Protection Laws.

2.3 The Supplier shall only process Protected Data for the purposes of the provision of the Services and for the specific purposes in each case as set out in Annex 1 (Details of Processing of Personal Data) to this Addendum and shall not process, transfer, modify, amend or alter the Protected Data or disclose or permit the disclosure of the Protected Data to any third party other than in accordance with the Customer's documented instructions (whether in the Main Agreement or otherwise) unless required to do so by applicable law to which the Supplier is subject; in such case the Supplier shall inform the

Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.4 The Supplier shall immediately inform the Customer if, in its opinion, an instruction pursuant to the Main Agreement or this Addendum infringes Data Protection Laws.

2.5 The Customer warrants to and undertakes with the Supplier that all data subjects of the Protected Data have been or will be provided with appropriate notices and information to establish and maintain for the relevant term the necessary legal grounds under Data Protection Laws for transferring the Protected Data to the Supplier to enable the Supplier to process the Protected Data in accordance with this Addendum and the Main Agreement.

3. PROCESSOR PERSONNEL

3.1 The Supplier shall treat all Protected Data as strictly confidential and shall inform all its employees, agents, contractors and Sub-processors engaged in processing the Protected Data of the confidential nature of such Protected Data.

3.2 The Supplier shall take reasonable steps to ensure the reliability of any employee, agent, contractor and Sub-processor who may have access to the Protected Data, ensuring in each case that access is limited to those persons or parties who need to access the relevant Protected Data, as necessary for the purposes set out in section 2.1 above in the context of that person's or party's duties to the Supplier.

3.3 The Supplier shall ensure that all such persons or parties involved in the processing of Protected Data are subject to:

3.3.1 confidentiality undertakings or are under an appropriate statutory obligation of confidentiality; and

3.3.2 user authentication processes when accessing the Protected Data.

4. SECURITY

4.1 The Supplier shall implement appropriate technical and organisational measures to ensure a level of security of the Protected Data appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Protected Data transmitted, stored or otherwise processed.

5. SUB-PROCESSING

5.1 Subject to section 5.2, the Supplier shall not engage any Sub-processor to process Protected Data other than with the general written authorisation of the Customer.

5.2 As at the date of the Main Agreement or (if later) implementation of this Addendum, the Customer hereby authorises the Supplier to engage those Sub-processors set out in Annex 2.

5.3 The Supplier shall inform the Customer of any intended changes concerning the addition or replacement of other Sub-processors, thereby giving the Customer the opportunity to object to such changes.

5.4 With respect to each Sub-processor, the Supplier shall:

5.4.1 carry out adequate due diligence on each Sub-processor to ensure that it is capable of providing the level of protection for the Protected Data as is required by this Addendum including without limitation sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of Data Protection Laws and this Addendum;

5.4.2 include terms in the contract between the Supplier and each Sub-processor which are equivalent to those set out in this Addendum, and shall supervise compliance therewith;

5.4.3 remain fully liable to the Customer for any failure by each Sub-processor to fulfil its obligations in relation to the Processing of any Protected Data.

6. DATA SUBJECT RIGHTS

6.1 The Supplier shall without undue delay, and in any case within three (3) working days, notify the Customer if it receives a request from a data subject under any Data Protection Laws in respect of Protected Data, including requests by a data subject to exercise the data subject's rights under Data Protection Laws, and shall provide full details of that request.

6.2 Taking into account the nature of the processing of Protected Data, the Supplier shall assist the Customer by appropriate technical and organisational measures, insofar as this is reasonably possible, to enable the Customer to comply with any such request by a data subject to exercise data subject rights under Data Protection Laws.

7. INCIDENT MANAGEMENT

7.1 In the case of a personal data breach involving Protected Data, the Supplier shall without undue delay notify the personal data breach to the Customer providing the Customer with sufficient information which allows the Customer to meet any obligations to report a personal data breach under Data Protection Laws. Such notification shall as a minimum:

7.1.1 describe the nature of the personal data breach, the categories and numbers of data subjects concerned, and the categories and numbers of Protected Data records concerned;

7.1.2 communicate the name and contact details of the Supplier's data protection officer or other relevant contact from whom more information may be obtained;

7.1.3 describe the likely consequences of the personal data breach; and

7.1.4 describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.2 The Supplier shall fully co-operate with the Customer and take such reasonable steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each personal data breach, in order to enable the Customer to *(i)* perform a thorough investigation into the personal data breach, *(ii)* formulate a correct response and to take suitable further steps in respect of the personal data breach in order to meet any requirement under Data Protection Laws.

7.3 The Supplier's obligation to report a personal data breach and assist the Customer under this Section will not be construed as an acknowledgment by the Supplier of any fault or liability with respect to the personal data breach.

7.4 The parties agree to coordinate and cooperate in good faith on developing the content of any related public statements or any required notices for the affected persons. The Supplier shall not inform any third party without first obtaining the Customer's prior written consent, unless notification is required by law to which the Supplier is subject, in which case the Supplier shall to the extent permitted by such law inform the Customer of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Customer before notifying the personal data breach.

8. DATA PROTECTION IMPACT ASSESSMENT

8.1 The Supplier shall, at the Customer's request, taking into account the nature of processing and the information available to the Supplier, provide reasonable assistance to the Customer with any data protection impact assessments and any consultations with any Supervisory Authority of the Customer as may be required in relation to the processing of Protected Data by the Supplier on behalf of the Customer.

9. DELETION OR RETURN OF PROTECTED DATA

9.1 Upon request made by the Customer within thirty (30) days of the earlier of: *(i)* cessation of processing of Protected Data by the Supplier; or *(ii)* termination of the Main Agreement, the Supplier shall return all Protected Data to the Customer. After such thirty (30) day period, the Supplier shall, at Customer's election, delete all Protected Data or return all Protected Data to the Customer.

9.2 If the Customer does not make an election within such thirty (30) day period, the Supplier shall securely dispose of Protected Data and delete all copies of it (except to the extent that any applicable law requires the Supplier to retain a copy of such Protected Data) and Customer acknowledges that the Supplier will have no obligation to maintain or provide such Protected Data.

10. AUDIT RIGHTS

10.1 The Supplier shall make available to the Customer on request all information necessary to demonstrate compliance with this Addendum and Data Protection Laws.

10.2 The Supplier shall permit the Customer or another auditor mandated by the Customer during normal working hours and on reasonable prior notice to inspect, audit and copy any relevant records, processes and systems in order that the Customer may satisfy itself that the provisions of Data Protection Laws and this Addendum are being complied with.

11. INTERNATIONAL TRANSFERS OF PROTECTED DATA

11.1 The Supplier shall not (permanently or temporarily) process the Protected Data nor permit any Sub-processor to (permanently or temporarily) process the Protected Data in a country outside of the UK or the EEA without an adequate level of protection, other than in respect of those recipients in such countries listed in Annex 3 (*Authorised Transfers of Protected Data*), unless authorised in writing by the Customer in advance.

11.2 When requested by the Customer, the Supplier shall promptly enter into (or procure that any relevant Sub-processor of the Supplier enters into) Standard Contractual Clauses in respect of any processing of Protected Data in a country outside of the UK or the EEA without an adequate level of protection.

12. LIABILITY

12.1 The disclaimers and limitations and exclusions of liability set out under the Main Agreement shall apply also to this Addendum.

13. COSTS

13.1 The Customer shall pay any reasonable costs and expenses incurred by the Supplier in meeting the Customer's requests made under this Addendum.

14. MISCELLANEOUS

14.1 Any obligation imposed on the Supplier under this Addendum in relation to the processing of Protected Data shall survive any termination or expiration of the Main Agreement.

14.2 With regard to the subject matter of this Addendum, in the event of any conflict or inconsistency between any provision of the Main Agreement and any provision of this Addendum, the provision of this Addendum shall prevail. In the event of any conflict or inconsistency between the Main Agreement or this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA

This Annex 1 includes certain details of the processing of personal data as required by Article 28(3) GDPR.

Subject matter and duration of the processing of personal data

The Supplier will process Personal Data to provide the Services. The duration of the processing will be the term of the Main Agreement.

The nature and purpose of the processing of personal data

CRB Cunninghams software products hold personal data sourced from the school MIS (or created manually), the data is used to verify the identity of an individual at the point of service delivery via computer terminals, EPOS terminals, Coin & Note revaluation units, self-service kiosks, registration terminals, printers, lockers and other similar devices within the customers site and allow them to use the services provided by that software.

The types of personal data to be processed

Commonly Held data includes: - Surname, Legal Surname, Forename, Registration Group, Year, Date of Birth, Gender (NI – Sex), Free Meal Eligibility, Admission Number, MISID, Photograph, Card Number, Biometric template*

Optionally held data includes: - Tutor, Address, Postcode, Telephone, Email, Dietary preferences, Parental Consent, Start Date, Leavers Date, Locker number, PIN Number, Active Directory User Name, UPN, Dietary needs*

Transactional data: - Purchases, credits, refunds, attendance data. These are related to personal records using a system generated identifier.

Biometric Data*: - Biometric data (fingerprints and facial templates) are stored as a series of data points, converted from images by a mathematical algorithm. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available. The level of detail stored in these data points is well below the level of detail needed for forensic identification of someone and would be completely inadmissible, both in terms of quality and legality, in court. The data points are encrypted before being stored.

The encryption standard used for encrypting the data points is AES 256 with the symmetric key being stored in RSA 2048 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standardwp.pdf The AES 256 encryption standard is used for storing top secret designated data by the American military and the NSA. Both AES and RSA are well used and commonly understood encryption standards that cannot be broken by brute force in a reasonable time.

* These are defined as sensitive data

The categories of data subject to whom the personal data relates

Pupils, Students, Employees and any visitors that require access to services.

ANNEX 2: AUTHORISED SUB-PROCESSORS

Microsoft Azure, Microsoft Campus, Thames Valley Park, Reading, Berkshire, RG6 1WG.

SendGrid, SendGrid, Inc., 1801 California Street, Suite 500, Denver, Colorado 80202, United States.

Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin.

Vesta Merchant Services (VMS), Stables 1, Howbery Park, Wallingford, Oxon, OX10 8BA, United Kingdom

ANNEX 3: AUTHORISED TRANSFERS OF CONTROLLER PERSONAL DATA

SendGrid, SendGrid, Inc., 1801 California Street, Suite 500, Denver, Colorado 80202, United States.

Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin.

Vesta Merchant Services (VMS), Stables 1, Howbery Park, Wallingford, Oxon, OX10 8BA, United Kingdom