DATA PROCESSOR ADDENDUM

Where Customer is subject to EU data protection laws, this Data Processor Addendum shall apply to the extent that Supplier processes personal data on Customer's behalf.

1. DEFINITIONS

1.1 The terms "process/processing", "data subject", "data processor", "data 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 "Authorised Sub-processors" means (a) those Sub-processors (if any) set out in Annex 2 (Authorised Sub-processors); and (b) any additional Sub-processors consented to in writing by the Customer in accordance with section 5.1;

1.4 "Customer" means the Customer or Licensee under the Main Agreement;

1.5 "Data Protection Laws"

1.5.1 The GDPR is an EU Regulation and, in principle, it will no longer apply to the UK from the end of the transition period. However, if you operate inside the UK, you will need to comply with UK data protection law. The government has said that it intends to incorporate the GDPR into UK data protection law from the end of the transition period – so in practice there will be little change to the core data protection principles, rights and obligations found in the GDPR.

1.5.2 The EU version of the GDPR may also still apply directly to Vesta Merchant Services if we operate in Europe, offer goods or services to individuals in Europe, or monitor the behaviour or individuals in Europe.

1.5.3 The GDPR will still apply to any organisations in Europe who send Vesta Merchant Services data, so we may need to help them decide how to transfer personal data to the UK in line with the GDPR.

1.5.4 The ICO will not be the regulator for any European-specific activities caught by the EU version of the GDPR, although they hope to continue working closely with European supervisory authorities.

1.5.5 What will the UK data Protection law be?

1.5.6 The Data Protection Act 2018 (DPA 2018), which currently supplements and tailors the GDPR within the UK, will continue to apply.

1.5.7 The provisions of the GDPR will be incorporated directly into UK law from the end of the transition period, to sit alongside the DPA 2018.

1.5.8 New DP exit regulations have been passed which will make technical amendments to the GDPR so that it works in a UK-only context from the end of the transition period.

1.6 "EEA" means the European Economic Area;

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

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

1.9 "Services" means the services described in the Main Agreement;

1.10 “Standard Contractual Clauses” means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these;

1.11 “Sub-processor” means any data processor (including any affiliate of the Supplier) appointed by the Supplier to process personal data on behalf of the Customer;

1.12 “Supervisory Authority” means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

1.13 “Supplier” means the Supplier or Licensor under the Main Agreement.

2. PROCESSING OF THE PERSONAL DATA

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

2.2 Each party shall at all times in relation to processing connected with the Main Agreement comply with Data Protection Laws.

2.3 The Supplier shall only process the types of Personal Data relating to the categories of data subjects for the purposes of the Main Agreement 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 Personal Data or disclose or permit the disclosure of the
Personal Data to any third party other than in accordance with the Customer’s documented instructions (whether in the Main Agreement or otherwise) unless processing is required by applicable 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 before processing that Personal Data.

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 Personal 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 Personal Data to the Supplier to enable the Supplier to process the Personal Data in accordance with this Addendum and the Main Agreement.

3. PROCESSOR PERSONNEL

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

3.2 The Supplier shall take reasonable steps to ensure the reliability of any employee, agent, contractor and/or Authorized Subprocessor who may have access to the Personal Data, ensuring in each case that access is limited to those persons or parties who need to access the relevant Personal 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 Personal 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 Personal Data.

4. SECURITY

4.1 The Supplier shall implement appropriate technical and organisational measures to ensure a level of security of the Personal 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 Personal Data transmitted, stored or otherwise processed.

5. SUB-PROCESSING

5.1 Subject to section 5.4, the Supplier shall not engage any Sub-processor to process Personal Data other than with the prior specific or general written authorisation of the Customer.

5.2 In the case of general written authorisation, the Supplier shall inform the Customer of any intended changes concerning the addition or replacement of other processors, thereby giving the Customer the opportunity to object to such changes.

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

5.3.1 carry out adequate due diligence on each Sub-processor to ensure that it is capable of providing the level of protection for the Personal 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;

5.3.2 include terms in the contract between the Supplier and each Sub-processor which are the same as those set out in this Addendum, and shall supervise compliance thereof;

5.3.3 insofar as that contract involves the transfer of Personal Data outside of the EEA, incorporate the Standard Contractual Clauses or such other mechanism as directed by the Customer into the contract between the Supplier and each Sub-processor to ensure the adequate protection of the transferred Personal Data, or such other arrangement as the Customer may approve as providing an adequate protection in respect of the processing of Personal Data in such third country(ies); and

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

5.4 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 (Authorised Sub-processors).

6. DATA SUBJECT RIGHTS

6.1.1 The regulation sets out out the following rights applicable to data subjects:

A. The right to be informed;

B. The right of access;

C. The right to rectification;

D. The right to erasure (also known as the ‘right to be forgotten’);

E. The right to restrict processing;

F. The right to data portability;

G. The right to object;

H. Rights with respect to automated decision-making and profiling.

6.1.2 Data Subject Access

6.1.3 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

6.1.4 All subject access requests received must be forwarded to either your business contact or David Jones the Company's data protection officer.

6.1.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

6.1.6 Rectification of Personal Data

6.1.7 If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

6.1.8 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

6.1.9 Erasure of Personal Data

6.1.10 Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:

A. It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;
B. The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
C. The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);
D. The personal data has been processed unlawfully;
E. The personal data needs to be erased in order for the Company to comply with a particular legal obligation.
F. The personal data is being held and processed for the purpose of providing information society services to a child.

6.1.11 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

6.1.12 In the event the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

6.1.13 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

6.1.14 Subject access request, (right to be forgotten):

A. The right is not absolute and only applies in certain circumstances.
B. When does the right to erasure not apply?
C. The right to erasure does not apply if processing is necessary for one of the following reasons:
D. to exercise the right of freedom of expression and information;

E. to comply with a legal obligation;
F. for the performance of a task carried out in the public interest or in the exercise of official authority;
G. for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
H. for the establishment, exercise, or defence of legal claims.

6.2 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 Personal Data, including requests by a data subject to exercise rights in chapter III of GDPR, and shall provide full details of that request.

6.3 The Supplier shall co-operate as reasonably requested by the Customer to enable the Customer to comply with any exercise of rights by a data subject under any Data Protection Laws in respect of Personal Data and to comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Personal Data or the Main Agreement, which shall include:

6.3.1 the provision of all information reasonably requested by the Customer within any reasonable timescale specified by the Customer in each case, including full details and copies of the complaint, communication or request and any Personal Data it holds in relation to a data subject;

6.3.2 where applicable, providing such assistance as is reasonably requested by the Customer to enable the Customer to comply with the relevant request within the timescales prescribed by Data Protection Laws; and

6.3.3 implementing any additional technical and organisational measures as may be reasonably required by the Customer to allow the Customer to respond effectively to relevant complaints, communications or requests.

7. INCIDENT MANAGEMENT

7.1 In the case of a personal data breach, 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 Personal 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 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 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 AND PRIOR CONSULTATION

8.1 The Supplier shall, at the Customer's request, 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 Personal Data by the Supplier on behalf of the Customer.

9. DELETION OR RETURN OF CONTROLLER PERSONAL DATA

9.1 The Supplier shall promptly and in any event within 90 (ninety) calendar days of the earlier of: (i) cessation of processing of Personal Data by the Supplier; or (ii) termination of the Main Agreement, at the choice of the Customer either return all Personal Data to the Customer or securely dispose of Personal Data (and thereafter promptly delete all existing copies of it) except to the extent that any applicable law requires the Supplier to store such Personal 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 and allow for and contribute to audits, including inspections by the Customer or another auditor mandated by the Customer of any premises where the processing of Personal Data takes place.

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.

10.3 The Supplier shall provide full co-operation to the Customer in respect of any such audit and shall at the request of the Customer, provide the Customer with evidence of compliance with its obligations under this Addendum and Data Protection Laws.

11. INTERNATIONAL TRANSFERS OF CONTROLLER PERSONAL DATA

11.1 The Supplier shall not (permanently or temporarily) process the Personal Data nor permit any Authorised Sub-processor to (permanently or temporarily) process the Personal Data in a country outside of 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 Personal 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) an agreement with the Customer on Standard Contractual Clauses and/or such variation as Data Protection Laws might require, in respect of any processing of Personal Data in a country outside of the EEA without an adequate level of protection.

12. LIABILITY

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

14. COSTS

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

15. MISCELLANEOUS

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

15.2 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

Tucasi will be the processor of personal data for customers under the legal basis of this signed contract. Tucasi will process personal data for the duration of the agreement, until cancelation of contract is received in writing at least 30 days prior renewal date.

The nature and purpose of the processing of Personal Data

Tucasi will process personal data as necessary to perform the services pursuant to the agreement, as further specified in the documentation, and as further instructed by customer in its use of the services.

The types of Personal Data to be processed

Customer may submit personal data to the services, the extent of which is determined and controlled by the customer in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- Forename, Surname, DoB, Address, telephone number, email address, mobile number, notes, Gender, Class, year, UPN, dietary preferences, entitlement to free meals, entitlement to pupil premium funding, leaving date, gift aid status, child care voucher scheme entitlement, attendance on trips, discounts, transactions & purchase history, cheque numbers, messages, attendance at Parents evening, cohort membership, meal history, session history, parental / guardian name, address, mobile number, email address, IP address.

The categories of data subject to whom the Personal Data relates

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Pupils, Attendee's and Users of Customer Services and Facilities
- Parents and Guardians
- Prospects & customers (who are natural persons)

ANNEX 2: AUTHORISED SUB-PROCESSORS

Sub-processors are authorised under a general written authorisation. A full list of individual sub-processors can be found here – https://tucasi.atlassian.net/wiki/spaces/SHC/pages/34340867. Tucasi will communicate any proposed changes to sub-processors that are authorised under this general written authorisation. Tucasi will communicate this via the email address provided by the data controller.

- Remote Access Tools – Tools that provide remote access for Tucasi support teams to assist users
- Secure data sharing tools – Tools that provide the facility for Tucasi and Customers to transfer data securely
- Data centre hosting – Service providers who provide server hosting/infrastructure
- Messaging Services – Service providers who provide messaging services such as email, SMS or push notification
- Data destruction services – Companies who provide secure erasure/destruction of data e.g. Disk and document shredding
- CRM / Information Management systems – Systems used by Tucasi to manage information e.g. ticketing system used by our support teams

ANNEX 3: AUTHORISED TRANSFERS OF CONTROLLER PERSONAL DATA

☐ None

The parties authorised signatures have duly executed this Addendum.

Customer: _____	Supplier: Tucasi Ltd
Signature: _____	Signature: *Steve Parrott*
Print Name: _____	Print Name: Steve Parrott
Title: _____	Title: Managing Director
Date: _____	Date: 01/11/2021

The rest of this page is deliberately left blank.