DATA PROCESSING AGREEMENT

This DPA is entered into between the Nesscomp Limited and the Customer and is incorporated into and governed by the terms of the Agreement.

1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Terms and Conditions.

"**Affiliates**"	means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;
"**Agreement**"	means the agreement between the Processor and the Controller for the provision of the Solution and Services;
"**Controller**"	means the Customer;
"**Data Protection Law**"	means the GDPR and/or any subsequent amendment or replacement or supplementary legislation;
"**Data Subject**"	shall have the same meaning as in Data Protection Law;
"**DPA**"	means this data processing agreement together with Exhibits A and B;
"**GDPR**"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;
"**Personal Data**"	shall have the same meaning as in Data Protection Law;
"**Processor**"	means Nesscomp Limited;
"**Standard Contractual Clauses**"	means the EU model clauses for personal data transfer from controllers to processors c2010-593 - Decision 2010/87EU;
"**Sub-Processor**"	means any person or entity engaged by the Processor or its Affiliate to process Personal Data in the provision of the Solution and Services to the Controller.

2. Purpose

2.1 The Processor has agreed to provide the Solution and Services to the Controller in accordance with the terms of the Agreement. In providing the Solution and Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. Scope

3.1 In providing the Solution and Services to the Controller pursuant to the terms of the Agreement, the Processor shall process Personal Data only to the extent necessary to provide the Solution and Services in accordance with both the terms of the Agreement and the Controller's instructions documented in the Agreement and this DPA.

4. Processor Obligations

4.1 The Processor may collect, process or use Personal Data only within the scope of this DPA.

4.2 The Processor confirms that it shall process Personal Data on behalf of the Controller and shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data shall only process the Personal Data on the documented instructions of the Controller.

4.3 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach any Data Protection Law.

4.4 The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

4.5 The Processor shall implement appropriate technical and organisational procedures to protect Personal Data, 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 risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.6 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of 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.

4.7 The technical and organisational measures detailed in Exhibit B shall be at all times adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA.

4.8 The Controller acknowledges and agrees that, in the course of providing the Solution and Services to the Controller, it may be necessary for the Processor to access the Personal Data to respond to any technical problems or Controller queries and to ensure the proper working of the Solution and Services. All such access by the Processor will be limited to those purposes.

4.9 Where Personal Data relating to an EU Data Subject is transferred outside of the EEA it shall be processed in accordance with the provisions of the Standard Contractual Clauses, unless the processing takes place: (i) in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) by an organisation located in a country which has other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

4.10 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.

4.11 The Processor confirms that it and/or its Affiliate(s) have appointed a data protection officer where such appointment is required by Data Protection Law. The appointed data protection officer may be reached at   dpo@nesscomp.com.

5. Controller Obligations

5.1 The Controller represents and warrants that it shall comply with the terms of the Agreement, this DPA and Data Protection Law.

5.2 The Controller represents and warrants that it has obtained any and all necessary permissions and authorisations necessary to permit the Processor, its Affiliates and Sub-Processors, to execute their rights or perform their obligations under this DPA.

5.3 The Controller is responsible for compliance with all Data Protection Law, including requirements with regards to the transfer of Personal Data under this DPA and the Agreement.

5.4   All Affiliates of the Controller who use the Solution and Services shall comply with the obligations of the Controller set out in this DPA.

5.5   The Controller shall implement appropriate technical and organisational procedures to protect Personal Data, 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 risk of varying likelihood and severity for the rights and freedoms of natural persons. The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security account shall be taken in particular of 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.

5.6   The Controller shall take steps to ensure that any natural person acting under the authority of the Controller who has access to Personal Data only processes the Personal Data on the documented instructions of the Controller.

5.7   The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Processor will process the request to the extent it is lawful, and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

5.8   The Controller acknowledges and agrees that some instructions from the Controller, including destruction or return of data, assisting with audits, inspections or DPIAs by the Processor, may result in additional fees. In such case, the Processor will notify the Controller of its fees for providing such assistance in advance, unless otherwise agreed.

6.   Sub-Processors

6.1   The Controller acknowledges and agrees that: (i) Affiliates of the Processor may be used as Sub-processors; and (ii) the Processor and its Affiliates respectively may engage Sub-processors in connection with the provision of the Solution and Services.

6.2   All Sub-processors who process Personal Data in the provision of the Solution and Services to the Controller shall comply with the obligations of the Processor set out in this DPA.

6.3   Where Sub-processors are located outside of the EEA, the Processor confirms that such Sub-processors: (i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) have entered into Standard Contractual Clauses with the Processor; or (iii) have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

6.4   The Processor shall make available to the Controller the current list of Sub-processors which shall include the identities of Sub-processors and their country of location. During the term of this DPA, the Processor shall provide the Controller with prior notification, via email, of any changes to the list of Sub-processor(s) who may process Personal Data before authorising any new or replacement Sub-processor(s) to process Personal Data in connection with the provision of the Solution and Services.

6.5   The Controller may object to the use of a new or replacement Sub-processor, by notifying the Processor promptly in writing within ten (10) Business Days after receipt of the Processor's notice. If the Controller objects to a new or replacement Sub-processor, the Controller may terminate the Agreement with respect to those parts of the Solution or Services which cannot be provided by the Processor without the use of the new or replacement Sub-processor. The Processor will refund the Controller any prepaid fees covering the remainder of the term of the Agreement following the effective date of termination with respect to such terminated Solutions or Services.

7.   Liability

7.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

7.2 The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

7.3 The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Controller itself.

7.4 The Controller shall not be entitled to recover more than once in respect of the same claim.

8. Audit

8.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

8.2 Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may conduct a more extensive audit which will be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance; (iii) carried out during UK business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Processor's day-to-day business.

8.3 This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

9. Data Breach

9.1 The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("**Data Breach**").

9.2 The Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Data Breach, and to assist the Controller in meeting the Controller's obligations under applicable law.

10. Compliance, Cooperation and Response

10.1 In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.

10.2 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller, unless such notification is not permitted under applicable law or a relevant court order.

10.3 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.

10.4 The Processor shall reasonably assist the Controller in meeting its obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of processing and the information available to the Processor.

10.5 The parties acknowledge that it is the duty of the Controller to notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the parties

agree that amendments are required, but the Processor is unable to accommodate the necessary changes, the Controller may terminate the part or parts of the Solution or Services which give rise to the non-compliance. To the extent that other parts of the Solution or Services provided are not affected by such changes, the provision of those Solutions or Services shall remain unaffected.

10.6   The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA.

11.   Term and Termination

11.1   The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

11.2   The Processor shall at the choice of the Controller, upon receipt of a written request received within 30 days the end of the provision of the Solution and Services relating to processing, delete or return Personal Data to the Controller. The Processor shall in any event delete all copies of Personal Data in its systems within 60 days of the effective date of termination of the Agreement unless: (i) applicable law or regulations require storage of the Personal Data after termination; or (ii) partial Personal Data of the Customer is stored in backups, then such Personal Data shall be deleted from backups up 1 year after the effective date of termination of the Agreement.

12.   General

12.1   This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

12.2   Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

12.3   This DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

Exhibit A

Overview of data processing activities to be performed by the Processor

1.   Controller

The Controller transfers Personal Data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below.

The Controller is the Customer.

2.   Processor

The Processor received data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below.

The Processor is Nesscomp Limited.

3.   Data Subjects

The Personal Data transferred includes but is not limited to the following categories of Data Subjects:

- Children, parents and guardians of the school managed by the Controller
- Employees, volunteers, freelancers and contractors of the Controller, and other users added by the Controller from time to time.
- Users, Affiliates and other participants from time to time to whom the Controller has granted the right to access the Solution and Services in accordance with the terms of the Agreement.

4.   Categories of Data

The Personal Data transferred includes but is not limited to the following categories of data:

- Personal details, names, user names, passwords, email addresses of Authorised Users.
- Personal Data derived from Authorised User's use of the Solution and Services such as records and business intelligence information.
- Personal Data within email and messaging content which identifies or may reasonably be used to identify, data subjects.
- Meta data including sent, to, from, date, time, subject, which may include Personal Data.
- Financial data.
- Data concerning education and profession.
- File attachments that may contain Personal Data.
- Survey, feedback and assessment messages.
- Information offered by users as part of support enquiries.
- Other data added by the Controller from time to time.

5.   Special categories of Data

Personal Data transferred includes but is not limited to the following special categories of data:

- Data relating to children special health needs.

6.   Processing operations

The Personal Data transferred will be subject to the following basic processing activities:

- Personal Data will be processed to the extent necessary to provide the Solution and Services in accordance with both the Agreement and the Controller's instructions. The Processor processes Personal Data only on behalf of the Controller.
- Processing operations include but are not limited to: students', parent's and guardians' administration, administration of parental duties for the school, management of employees and intermediaries, monitoring of the workplace, client management, appraisals, performance reviews, feedback, objectives and personal development tracking, making comments and updates on these, management of lists of students, parents, employees, intermediaries and other users, providing support to user and other HR functions, etc. These operations relate to all aspects of Personal Data processed.
- Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical issues both generally in the provision of the Solution and Services and specifically in answer to a Controller query. This operation may relate to all aspects of Personal Data processed but will be limited to metadata where possible.

Technical and Organisational Security Measures

The following descriptions provide an overview of the technical and organisational security measures implemented. It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available. It's acknowledged and agreed that the technical and organisational measures described therein will be updated and amended from time to time, at the sole discretion of the Processor.

1.   Entrance Control

Technical or organisational measures regarding access control, especially regarding legitimation of authorised persons:

The aim of the entrance control is to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Personal Data.

Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorisations. Main entrance is monitored by security personnel. Access for employees is only possible with an encoded ID and through security enabled access door.

2.   System Access Control

Technical and organisational measures regarding the user ID and authentication:

The aim of the system access control is to prevent unauthorised use of data processing systems, are used for the processing of Customer Data.

Remote access to the data processing systems is only possible through the Processor's secure VPN tunnel. If the users first authenticate to the secure VPN tunnel, after successful authentication authorisation is executed by providing a unique user name and password to a centralised directory service. All access attempts, successful and unsuccessful are logged and monitored.

Additional technical protections are in place using firewalls.

3.   Data Access Control

Technical and organisational measures regarding the on-demand structure of the authorisation concept, data access rights and monitoring and recording of the same:

Measures regarding data access control are targeted on the basis that only such data can be accessed for which an access authorisation exists and that data cannot be read, copied, changed or deleted in an unauthorised manner during the processing and after the saving of such data.

Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance to the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person.

To maintain data access control, state of the art encryption technology is applied to the Personal Data itself where deemed appropriate to protect sensitive data based on risk.

4.   Transmission Control

Technical and organisational measures regarding the transport, transfer, transmission, storage and subsequent review of Personal Data on data media (manually or electronically).

Transmission control is implemented so that Personal Data cannot be read, copied, changed or deleted without authorisation, during transfer or while stored on data media, and so that it can be monitored and determined as to which recipients a transfer of Personal Data is intended.

For the purpose of transfer control, an encryption technology is used (e.g. remote access to the company network via VPN tunnel and full disk encryption). The suitability of an encryption technology is measured against the protective purpose.

The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers). is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred to companies located outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the Standard Contractual Clauses.

5.   Data Entry Control

Technical and organisational measures regarding recording and monitoring of the circumstances of data entry to enable retroactive review.

System inputs are recorded in the form of log files therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted.

6.   Data Processing Control

Technical and organisational measures to differentiate between the competences of principal and contractor:

The aim of the data processing control is to provide that Personal Data is processed by a commissioned data processor in accordance with the Instructions of the principal.

Details regarding data processing control are set forth in the Agreement and DPA.

7.   Availability Control

Technical and organisational measures regarding data backup (physical/logical):

If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.

8.   Separation Control

Technical and organisational measures regarding purposes of collection and separated processing:

Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems.

Customer Data is stored in a way that logically separates it from other customer data.

The Controller's archived data is encrypted at rest using AES256 bit encryption and data in transit is protected by Transport Layer Security ("TLS").