Data Processing Addendum

If you are subject to the European Union Data Protection Directive 95/46/EC, or similar statute, the terms of this Data Processing Addendum ("DPA") are incorporated by reference to the Master Agreement between you and Blackboard (the "Agreement").

Data Processing Clauses

The following provisions shall apply whenever Customer Data are processed on your behalf:

1. Blackboard’s obligations

1.1 Blackboard shall process data and information provided by you or your Authorized End Users ("Customer Data") within the scope of the Agreement, for the purpose of service provision during the term of the Agreement, and pursuant to your instructions. We shall not compile copies or duplicates without your approval, except for copies made for backup or disaster recovery purposes.

1.2 Annex A of this DPA contains a list of the categories of Customer Data and the data subjects concerned.

2. Authority to issue instructions

2.1 We agree, without limitation, to strictly follow any instructions given by you under the Agreement as well as those issued on an individual basis with regard to the collection, processing and/or usage of Customer Data. This includes but is not limited to instructions on the blocking, correction or deletion of Customer Data. Our obligations under this Section 2.1 shall be subject to Section 2.3.

2.2 Instructions may only be issued by your management board, data protection officers or the manager of your legal department, if applicable (hereinafter "persons authorized to issue instructions"). The persons authorized to issue instructions shall have the right, at all times, to make written appointments of additional persons authorized to issue instructions.

2.3 If we hold the view that any instruction of yours contravene statutory regulations and/or the Agreement, we will notify you immediately, and we are entitled to suspend execution of the instruction concerned, until you confirm such instruction in writing. We have the right to deny the execution of an instruction – even if issued in writing – in case we would be liable under applicable law if we execute the instruction.

2.4 We shall, by way of regular self-audits, ensure that the processing of Customer Data on your behalf conforms to this DPA and any instructions issued by you.

3. Data secrecy

3.1 We undertake to maintain data secrecy, pursuant to applicable law, and keep Customer Data confidential.

3.2 We confirm that we are aware of the applicable data protection regulations. We agree that we make our applicable employees familiar with the relevant provisions of data protection regulations. We shall supervise compliance of such employees with applicable data protection regulations.

4. Sub-Processing

4.1 In accordance with the provisions of this DPA and the Agreement, you acknowledge and agree that Blackboard or Blackboard affiliates (which are hereby designated as sub-processors for the purpose of processing Customer Data) ("Blackboard Affiliates") may store or process Customer
Data in various data centers around the world and that Customer Data might not be hosted within the country in which you are located. Upon your request, we will tell you where Customer Data is located. Notwithstanding anything to the contrary in this Section, if we and you have agreed that Customer Data will be stored in any particular location, we will store such Customer Data in the agreed location.

4.2 If your Agreement is with a Blackboard entity located in the European Economic Area ("EEA"), we have entered into a data transfer agreement based on the European Standard Contractual Clauses for Processors (the "Model Clauses") with Blackboard Affiliates based outside the EEA that receive Customer Data.

(a) If you request, Blackboard agrees to conclude a specific data transfer agreement based on the Model Clauses with those Blackboard Affiliates located outside the EEA as agent for you and you authorize us to act in your name for this purpose. In such case, the provisions of this DPA apply in addition to those of such data transfer agreement and, in the case of any conflict, the provisions under the specific data transfer agreement will prevail.

(b) If you request and only to the extent legally required, we will have the Blackboard Affiliates located outside of the EEA conclude a direct data transfer agreement based on the Model Clauses with you.

4.3 If your Agreement is with Blackboard Inc. or another Blackboard entity located outside the EEA, at your request and to the extent legally required, we agree to conclude a data transfer agreement based on the Model Clauses with you.

4.4 You consent to allow us to provide access to Customer Data to certain third party service providers that need to access such information in order to provide their services to us as part of our provision of the Products and Services to you. Our third party service providers are required to maintain the confidentiality of such information and we enter into agreements with service providers that are either based on the Model Clauses (if needed) or that contain other privacy and security protections which do not fall below the level of data protection provided by this DPA.

5. Audit

5.1 Upon request, we will provide you an overview of our data processing operations, to include the following information:

(a) owners, managing boards, managing directors or other lawfully or constitutionally appointed managers and the persons placed in charge of the Customer Data processing;

(b) our address;

(c) purposes of collecting, processing or using the Customer Data;

(d) a description of the groups of data subjects and the Customer Data or categories of Customer Data;

(e) recipients or categories of recipients to whom the Customer Data may be transferred;

(f) standard periods for the retention of Customer Data;

(g) any planned data transfer to third countries; and
(h) a general description enabling a preliminary assessment as to whether the technical and organizational measures to guarantee the safety of processing are adequate.

The Parties agree and acknowledge that for the purposes of this Section 5.1 it shall be sufficient that we present all documentation, including a certified statement on the compliance with this Agreement, in such format as reasonably required by you or any independent auditor appointed by you at your expense.

5.2 You have the right to audit our compliance with the statutory regulations on data protection and the stipulations entered into between the Parties (including the technical and organizational measures), by requesting information about and inspecting storage of the Customer Data, and implemented policies and security incident reports, subject to reasonable prior notice of at least 14 days in advance and, to the extent reasonably possible, without interfering with our regular business operations.

6. Data security measures

6.1 We use the following appropriate technical and organizational measures to protect Customer Data, which have to meet, at a minimum, the level required by applicable law:

(a) Admission control:
- We employ appropriate physical safeguards to prevent unauthorized persons from gaining access to the premises where Customer Data is collected, processed and used. Such premises may only be entered by us and/or our agents.
- We use appropriate measures to secure buildings.
- We use appropriate measures to ensure that Customer Data held in hardcopy are kept securely e.g. in locked rooms or filing cabinet. Generally, steps are taken to ensure that access to hardcopy Customer Data is limited in the same way it would be on an electronic IT system i.e. access is limited to those individuals where it is necessary for them to have access in order for them to perform their job role.

(b) Entry control:
- We shall endeavour to prevent unauthorized parties from accessing or using our data processing systems.
- We shall require authentication and authorisation to gain access to IT systems (i.e. require users to enter a user id and password before they are permitted access to IT systems).
- We have procedures in place to permit only authorized persons to access Customer Data internally or externally by using authentication procedures (e.g. by means of appropriate passwords), except as otherwise enabled by you.

(c) Access control:
- We employ appropriate measures to prevent individuals accessing Customer Data unless they hold a specific access authorization.
- We employ appropriate measures to only permit user access to Customer Data which the user needs to access for his/her job role or the purpose they are given access to our IT systems for (i.e. we implement measures to ensure least privilege access to IT systems).
- We shall have in place appropriate procedures for controlling the allocation and revocation of Customer Data access rights. For example, having in place appropriate procedures for revoking employee access to IT systems when they leave their job or change role.

- Our systems that are used to collect, process and use Customer Data are protected by user identifiers, passwords and graded access rights. Special access rights are produced for the purposes of technical maintenance which do not allow access to Customer Data.

- We take appropriate administrative safeguards to protect our services against external attacks, including, for example, deploying firewalls.

(d) Transmission control:

- We shall employ appropriate measures to ensure that Customer Data cannot be read, copied, altered or removed without authorization during electronic transmission.

- We shall employ encryption technology while in motion to protect Customer Data held electronically.

(e) Input control:

- We maintain logging and auditing systems to monitor activity related to the input of Customer Data.

(f) Order control:

- We shall ensure that all requests from you with respect to Customer Data shall be processed strictly in compliance with your instructions through the use of clear and unambiguous contract terms; comprehensive Statements of Work; and/or monitoring of contract performance.

(g) Availability control:

- We shall protect Customer Data in our possession against unintentional destruction or loss through a series of technical and procedural measures including firewall systems; monitoring; and back-up procedures.

- Examples measures that may also be taken include: mirroring of storage media, uninterruptible power supply (UPS); remote storage; firewall systems; and disaster recovery plans.

6.2 The technical and organizational measures described in Section 6.1 are subject to technological advancements and further development. We are permitted to implement suitable alternative measures, as long as the alternative measures do not reduce the level of security applied to the Customer Data.

6.3 We shall regularly audit and assess our compliance with the technical and organizational security measures.

7. Notification duties

7.1 Notification of infringements of data protection regulations
(a) We shall notify you to the extent the technical and organizational measures taken by us are not in accordance with this DPA or your instructions. The same applies to malfunctions or indications for an infringement of data protection regulations, or in case of improper processing of Customer Data, including, but not limited to, data security breaches and data losses. We and you shall mutually agree on any further collection, processing and usage of Customer Data, and we shall initiate all reasonably necessary measures to exclude risks to the integrity and confidentiality of Customer Data.

(b) In the event we have a reasonable, good faith belief that an unauthorized third party has gained access to or disclosed Customer Data, we will promptly, or if required by Law in such other time required by such Law, notify you. We will provide you with reasonable cooperation and assistance in relation to your investigation of the incident. If such incident triggers any third-party notice requirements under Laws, you agree that unless otherwise required by Law, as the owner of the Customer Data, you will be responsible for the timing, content, cost and method of any such notice and compliance with such Laws.

7.2 We shall notify you about:

(a) any legally binding request for disclosure of the Customer Data by a law enforcement authority or other organization or body, unless prohibited by law;

(b) any request received directly by us from a data subject.

7.3 We agree to provide you with reasonable cooperation and assistance in relation to any request under Section 7.2.

8. Deletion of data

8.1 Upon expiration or earlier termination of the processing services, or such earlier time as you request, we agree, at your request, to:

(a) return to you or your designee; or

(b) securely destroy or render unreadable or undecipherable,

the relevant Customer Data in our possession, custody or control.

8.2 We shall ensure from an organizational perspective that Customer Data can be deleted within a reasonable time frame consistent with your request or deletion requirements established in the Agreement, except that we shall not be obliged to delete Customer Data from archival and back-up files except as in line with our company data deletion schedule. If you request deletion of Customer Data in archival and back-up-files, you shall bear the costs including costs for business interruptions associated with such request.


9.1 Unless specifically stipulated to the contrary by the Parties, the duration of the commissioned data processing specified by this DPA shall be coterminous with the term of the Agreement.

9.2 In the event of a conflict between this DPA and any other provision of the Agreement between you and us, this DPA will prevail; provided that if you and we have agreed in an Order Form to any terms that are different from this DPA, the terms in such Order Form will prevail.
Annex A – Details of the Data Processing

Categories of Data

<table>
<thead>
<tr>
<th>Name or unique identifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal contact information</td>
</tr>
<tr>
<td>Date of birth, Gender, Nationality, Parent/Student Relationships</td>
</tr>
<tr>
<td>Grade Level, Teachers, Classes/Sections/Courses, Grades, Assignments, Tests, Books, Attendance, Homework, Degree Type</td>
</tr>
<tr>
<td>Financial details</td>
</tr>
<tr>
<td>Usernames, passwords</td>
</tr>
<tr>
<td>Service or browsing history, Location data, information provided by social networks, User or Customer Correspondence</td>
</tr>
<tr>
<td>Disciplinary and conduct records</td>
</tr>
<tr>
<td>Any information contained in the submitted paper, assignment, or other user-generated content</td>
</tr>
</tbody>
</table>

Special Categories of Data (if any)

| Information relating to disability and health |
| Information relating to racial or ethnic origin |

Categories of Data Subject

| Customer and Customer’s Users authorized by Customer to use the Blackboard Services (Students, Teachers and Administrators) |