DATA PROCESSING AGREEMENT

PART 1 – PROCESSING DETAILS

Date	*[***]*
Applicable Services	
Customer	*[***]*
Services	*[***]*
Agreement	*[NAME OF THE AGREEMENT]*
Contact points for data protection queries	
Amplify	*Inna Barmash, General Counsel*
Customer	*[***]*

PART 1 – PROCESSING TERMS

BACKGROUND

Amplify Education, Inc ("**Amplify**") and Customer identified above entered into the **Agreement**.

Amplify may be granted access to personal data in the course of providing the Services to the Customer. To the extent that personal data relates to data subjects in the EEA or the UK (each as defined below) or where the Customer is established in the EEA or the UK, the Parties have agreed that this data protection agreement ("**DPA**") shall apply to the transfer of such personal data by the Customer to Amplify.

In the event of any conflict between the Agreement and this DPA, the provisions of this DPA shall prevail.

1. DEFINITIONS AND INTERPRETATION

1.1 In this DPA, unless expressly stated otherwise, the words below or capitalised terms used in this DPA shall have the meaning defined below, elsewhere in the DPA or in the Agreement:

"**Agreement**" has the meaning given to it in the Background;

"**Customer**" means the person identified in Part 1 of this DPA;

"**Customer Personal Data**" means the personal data described in Part 2 of this DPA and any other personal data that Amplify processes as a processor on behalf of the Customer in connection with Amplify's provision of the Services;

"**Data Protection Laws**" means the GDPR and all applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of personal data;

“De-identified Data” means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, household, or device;

"**DPA**" has the meaning given to it in the Background;

"**European Economic Area**" or "**EEA**" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein;

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council or, where applicable, the "UK GDPR" as defined in The Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019;

"**Objection**" has the meaning given to it in clause 7.3;

"**Party**" means each of the Customer and Amplify;

"**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Shared Personal Data or Customer Personal Data;

"**Services**" means the services provided to the Customer under the Agreement.

"**Shared Personal Data**" means the personal data described in Part 2 of this DPA that each Party processes as an independent controller;

"**Subprocessor**" means any processor engaged by Amplify that agrees to receive from Amplify Customer Personal Data.

1.2 The terms "**personal data**", "**controller**", "**processor**", "**data subject**", "**process**" and "**supervisory authority**" shall have the same meaning as set out in Data Protection Laws. Personal data does not include De-identified Data.

1.3 To the extent of any ambiguity or conflict, this DPA shall prevail over the Agreement.

2. ROLES AND RESPONSIBILITIES OF PARTIES

The following provisions apply to the extent that the concepts of “data controller” and “data processor” (or equivalent) exist under applicable Data Protection Laws.

2.1 **Independent Controllers.** Each Party (“Controller Party”) acknowledges that it is an independent controller with respect to Shared Personal Data.

2.2 **Amplify as Processor.** The parties acknowledge that Customer and/or its relevant Affiliates act as the Controller of the Customer Personal Data Processed by Amplify in its provision of the Services, and Amplify acts as the Processor of such Customer Personal Data. Amplify acknowledges and agrees that between Amplify and Customer, Customer owns all Customer Personal Data.

3. PROCESSING OF SHARED PERSONAL DATA

The Customer shall comply with all applicable Data Protection Laws with respect to the transfer of the Shared Personal Data to Amplify, including (without limitation):

3.1 providing all applicable notices to data subjects required under applicable Data Protection Laws; and

3.2 obtaining any consents required under applicable Data Protection Laws, in each case as required for the lawful processing of Shared Personal Data by Amplify in connection with its product development, research and analytics.

4. INTERNATIONAL TRANSFERS

4.1 Amplify shall transfer and otherwise Process personal data included in Shared Personal Data and Customer Personal Data belonging to a data subject within the European Economic Area ("EEA") and the United Kingdom ("UK"), including by any Subprocessor, in compliance with applicable Data Protection Laws.

(a) For transfers of personal data subject to Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR"), the standard contractual clauses issued pursuant to EU Commission Decision 2021/914/EU of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj, (the "SCCs") will apply; and

(b) For transfers of personal data subject to the UK's Data Protection Act 1998 ("UK Data Protection Law"), where the Parties are lawfully permitted to rely on the SCCs for transfers of personal data protected by UK Data Protection Law subject to completion of a UK Addendum to the European Commission Standard Contractual Clauses issued by the Information Commissioner's Office ("ICO") under or pursuant to section 119(A)(1) of the UK Data Protection Law, then the Parties agree that the SCCs and Part 5 ("UK Addendum") of this DPA shall apply or the Parties may mutually agree to amend Part 5 to reflect updated guidance from the ICO. If the UK Data Protection Law changes to require either a specific method of relying on the SCCs (such as an addendum that makes reference to laws, courts, and authorities in that jurisdiction) or use of a different form of Standard Contractual Clauses (or an equivalent agreement), the Parties will update Part 5 to implement an approach that is valid under the updated UK Data Protection Law for Personal Information that is subject to it.

4.2 The SCCs, together with Parts 1, 2, 3, 4, and 5 attached hereto, shall be deemed to be incorporated by reference into this DPA and to apply for the benefit of both parties, in accordance with the following:

(a) The signatories to this DPA are deemed to have signed the SCCs, which form part of this DPA and will be deemed completed as follows:

(i) Module 1 of the SCCs applies to transfers of Shared Personal Data from Customer to Amplify, and Module 2 of the SCCs applies to transfers of Customer Personal Data from Customer to Amplify;

(ii) Clause 7 of Modules 1 and 2 (the optional docking clause) is not included;

(iii) Under Clause 9 of Module 2 (Use of sub-processors), the Parties select Option 2 (General Written Authorisation). The agreed list of sub-processors is set forth in Part 3 (List of Subprocessors) of this Agreement and Amplify shall propose an update to that list at least 30 days in advance of any requested additions or replacements of sub-processors;

(iv) Under Clause 11 of Modules 1 and 2 (Redress), the optional language requiring that data subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;

(v) Under Clause 17 of Modules 1 and 2 (Governing law), these SCCs shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of [SPECIFY MEMBER STATE];

(vi) Under Clause 18 of Modules 1 and 2 (Choice of forum and jurisdiction), the Parties select the courts of the [SPECIFY MEMBER STATE];

(vii) Annex I(A) (List of Parties) and Annex I(B) (Description of Transfer) of Modules 1 and 2 are completed as set forth in Part 2 (Processing Details) of this Agreement;

(viii) Under Annex I(C) (Competent supervisory authority) of Modules 1 and 2, the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the competent supervisory authority as set forth in Part 2 (Processing Details);

(ix) Annex II of Modules 1 and 2 (Technical and organizational measures) is completed as set forth in Part 4 (Technical and Organizational Security Measures); and

(x) Annex III of Module 2 (List of sub-processors) is completed as set forth in Part 3 (Amplify's Existing Sub-processors) of this DPA.

4.3 Order of Applicability. To the extent the SCCs apply, nothing in this DPA or the Agreement shall be construed to prevail over any conflicting clause of the SCCs. Each party acknowledges that it has had the opportunity to review the SCCs.

4.4 Supplementary Measures. In addition to the obligations under Section 4.2 above, if and to the extent that the Parties will engage in cross-border Processing of personal data or will transmit, directly or indirectly, any personal data to a country outside of the country from which such personal data was collected (including without limitation transfers of personal data outside of the EEA and the UK), the parties agree to the following supplementary measures:

(a) The obligations in Modules 1 and 2 of Section III of the SCCs (Local laws and obligations in case of access by public authorities) shall form part of this DPA with respect to personal data subject to UK Data Protection Law, regardless of whether the rest of the SCCs apply to any personal data;

(b) Amplify warrants and represents that, as of the date of the Agreement, it has not received any national security data production orders (e.g., pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA Section 702") or U.S. Presidential Policy Directive 28).

(c) Amplify will resist, to the extent permitted by applicable law, any request under FISA Section 702 for surveillance whereby a targeted account is not uniquely identified;

(d) Amplify will use all available legal mechanisms to challenge any demands for data access through the national security process that Amplify receives; and

(e) No later than the effective date of the Agreement that incorporates or references this DPA, Amplify will either publish, at six month intervals, a transparency report indicating the types of binding legal demands for the personal data it has received, including national security orders and directives, which shall encompass any process issued under FISA Section 702, or notify Customer of any binding legal demand for the personal data it has received, including national security orders and directives, which shall encompass any process issued under FISA Section 702.

5. DISCLOSURE OF DATA TO NATIONAL AUTHORITIES

5.1 Amplify shall promptly notify the Customer, unless prohibited under applicable law, if it:

(a) receives any legally binding request from a public authority in the United States for disclosure of any Customer Personal Data or Shared Personal Data, and such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided;

(b) becomes aware of any direct access by public authorities in the United States to Customer Personal Data or Shared Personal Data; such notification shall include all information available to Amplify.

5.2 In the event that Amplify receives a request from a public authority in the United States for disclosure of any Customer Personal Data or Shared Personal Data, it shall:

(a) review, under applicable law, the legality of the request for disclosure, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if, after a careful assessment, it concludes that there are grounds under the laws of the country of destination to do so. When challenging a request, the data importer shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules;

(b) document its legal assessment as well as any challenge to the request for disclosure and, to the extent permissible under applicable law, make it available to the Customer and the competent supervisory authority upon request;

(c) provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

5.3 If Amplify is prohibited from notifying the Customer of a disclosure request received from a public authority, Amplify agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicate as much information and as soon as possible. Amplify agrees to document its best efforts in order to be able to demonstrate them upon request of the Customer.

5.4 To the extent permissible under applicable law, Amplify agrees to provide the Customer with regular updates regarding requests received from a public authorities including details of:

(a) the number of requests received;

(b) the types of data requested;

(c) the requesting authority;

(d) whether the requests have been challenged and the outcome of such challenges.

5.5 Amplify shall preserve the information set out in clauses 5.1, 5.2 and 5.4 for the duration of the Agreement and, to the extent permitted under applicable law, make it available to the competent supervisory authority upon request.

6. INSTRUCTIONS FOR DATA PROCESSING

6.1 Amplify shall only process the Customer Personal Data as required to provide the Services, unless processing of the Customer Personal Data is otherwise required by applicable law in the UK, the European Union or a Member State, in each case to which Amplify is subject, in which case Amplify shall, to the extent permitted by such applicable law, inform the Customer of that legal requirement before processing that Customer Personal Data.

6.2 Processing outside the scope of this DPA or the Agreement will require prior written agreement between the Customer and Amplify on additional instructions for processing.

6.3 The Customer represents and warrants that it has provided all applicable notices to data subjects and, to the extent required, obtained consent from data subjects in each case as required for the lawful processing of Customer Personal Data in accordance with the Agreement and this DPA.

6.4 In the event of a conflict between any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail.

7. SUBPROCESSORS

7.1 The Customer authorises Amplify to engage third parties as Subprocessors to process Customer Personal Data, including, provided it enters into a written agreement with the Subprocessor which:

(a) restricts the Subprocessor from processing the Customer Personal Data for any purposes other than the performance of the obligations subcontracted to it; and

(b) imposes the same obligations on the Subprocessor with regard to their processing of Customer Personal Data as are imposed on Amplify under this DPA.

7.2 Amplify shall provide the Customer with fourteen (14) days' notice of any proposed changes to the Subprocessors it uses to process Customer Personal Data (including any addition or replacement of any Subprocessors).

7.3 The Customer may, on reasonable grounds, object to Amplify's use of a new Subprocessor by providing Amplify with:

(a) written notice within seven (7) days after Amplify has provided notice to the Customer as described in clause 7.2; and

(b) documentary evidence that reasonably shows that the Subprocessor does not or cannot comply with the requirements in this DPA, (an "**Objection**").

7.4 In the event of an Objection, Amplify will use reasonable endeavours to make available to the Customer a change in the Services, or will recommend a commercially reasonable change to the Services to prevent the applicable Subprocessor from processing the Customer Personal Data. If Amplify is unable to make available such a change within a reasonable period of time, which shall not exceed thirty (30) days, either Party may terminate, without penalty, the Agreement by providing written notice to the other Party.

8. DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

8.1 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, Amplify shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

8.2 The Customer may audit (by itself or using independent third party auditors) Amplify's compliance with the security measures set out in this DPA, including by conducting audits of Amplify's (and Suprocessors') data processing facilities. Amplify shall assist with, and contribute to, any audits conducted in accordance with this clause 8.2, provided that:

(a) such audits are carried out during Amplify's normal working hours;

(b) such audits are not carried out more than once a year; and

(c) the Customer reimburses Amplify any costs and expense incurred by Amplify in facilitating the audit of its and its Subprocessors' data processing facilities.

8.3 Amplify shall make available to the Customer on request all information necessary to demonstrate compliance with this DPA. Where applicable by virtue of Article 28(3)(h) of the GDPR, Amplify shall immediately inform the Customer if, in its opinion, an instruction pursuant to clause 8.2 or clause 8.3 infringes applicable Data Protection Laws.

8.4 If Amplify or any Subprocessor becomes aware of, or has reason to suspect that there has been, a Security Incident, Amplify will:

(a) notify the Customer of the Security Incident without undue delay;

(b) investigate the Security Incident and provide such reasonable assistance to the Customer (and any law enforcement or regulatory official) as required to investigate the Security Incident, and

(c) take steps to remedy any non-compliance with this DPA.

8.5 Amplify shall treat the Customer Personal Data as the confidential information of the Customer, and shall ensure that:

(a) access to Customer Personal Data is limited to those employees or other personnel who have a business need to have access to such Customer Personal Data;

(b) any employees or other personnel have agreed in writing to protect the confidentiality and security of Customer Personal Data.

9. DATA SUBJECT RIGHTS

9.1 Save as required (or where prohibited) under applicable law, Amplify shall notify the Customer of any request received by Amplify or any Subprocessor from a data subject in respect of their personal data included in the Customer Personal Data, and shall not respond to the data subject.

9.2 Amplify shall, where possible, assist the Customer with ensuring its compliance under applicable Data Protection Laws, and in particular shall:

(a) taking into account the nature of the processing, provide the Customer with the ability to correct, delete, block, access or copy the personal data of a data subject (insofar as this is possible), or

(b) promptly correct, delete, block, access or copy Customer Personal Data within the Amplify Service at the Customer's request.

9.3 Amplify shall notify the Customer of any request for the disclosure of Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency.

10. ASSISTANCE

10.1 Where applicable, taking into account the nature of the processing, and to the extent required under applicable Data Protection Laws, Amplify shall:

(a) use all reasonable endeavours to assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising Data Subject rights laid down in the GDPR; and

(b) provide reasonable assistance to the Customer with any data protection impact assessments and with any prior consultations to any supervisory authority of the Customer, in each case solely in relation to processing of Customer Personal Data and taking into account the information available to Amplify.

11. INDEMNITY; LIMITATIONS ON LIABILITY

11.1 Any exclusions or limitations of liability set out in the Agreement shall apply to any losses suffered by either Party (whether in contract, tort (including negligence) or for restitution, or for breach of statutory duty or misrepresentation or otherwise) under this DPA as if this DPA was incorporated into, and formed a part of the Agreement.

12. DURATION AND TERMINATION

12.1 This DPA shall commence on the date of this DPA and shall continue until the date of termination or expiry of the Agreement.

12.2 Subject to clause 12.3 below, Amplify shall, within seven (7) days of the date of termination of the Agreement:

(a) if requested to do so by the Customer within that period, return a complete copy of all Customer Personal Data by secure file transfer in such a format as notified by the Customer to Amplify; and

(b) delete and use all reasonable efforts to procure the deletion of all other copies of Customer Personal Data processed by Amplify or any Subprocessors.

12.3 Amplify and its Subprocessors may retain Customer Personal Data to the extent required by applicable laws and only to the extent and for such period as required by applicable laws and always provided that Amplify shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

13. GENERAL

13.1 **Written Communications**. Applicable laws may require that some of the information or communications that the Parties send to each other should be in writing. The Parties agree, for the purposes of this DPA, that communication between them will mainly be electronic and that the Parties will contact each other by e-mail. For contractual purposes, the Parties agree to this electronic means of communication and the Parties acknowledge that all contracts, notices, information and other communications provided by one Party to the other electronically comply with any legal requirement that such communications be in writing.

13.2 **Notices.** Any notices given by one Party to the other will be served if validly served in accordance with the Agreement, and will be deemed received in accordance with the relevant provisions in the Agreement.

13.3 **Rights and remedies.** Except as expressly provided in the Agreement, the rights and remedies provided under the Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

13.4 **No partnership or agency.** Nothing in the DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the Parties, constitute any Party the agent of another Party, or authorise any Party to make or enter into any commitments for or on behalf of any other Party. Each Party confirms it is acting on its own behalf and not for the benefit of any other person.

13.5 **Transfer of rights and obligations**. Neither Party shall transfer, assign or otherwise deal in the DPA, or any of its rights and obligations under this DPA, other than to an assignee of that Party's rights and obligations under the Agreement.

13.6 **Third party rights.** Other than as expressly stated in the DPA, a person who is not a party to this DPA may not enforce any of its terms under the Contracts (Rights of Third Parties) Act 1999.

13.7 **Waiver**. No forbearance or delay by either Party in enforcing its rights shall prejudice or restrict the rights of that Party, and no waiver of any such rights or any breach of any contractual terms shall be deemed to be a waiver of any other right or of any later breach.

13.8 **Variation.** No variation of this DPA shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

13.9 **Severability**. If any provision of the DPA is judged to be illegal or unenforceable, the continuation in full force and effect of the remainder of the provisions of the DPA shall not be prejudiced.

13.10 **Law**. This DPA shall be governed by, and construed in accordance with, the law of the Member State where the Customer is established (or, where the Customer is established in the United Kingdom, English law).

The Parties have read and accept the terms and conditions of this DPA:

Signed for and on behalf of Amplify Education, Inc: _____ *Signature*	Signed for and on behalf of the Customer by: _____ *Signature*
Name:	Name:
Position:	Position:

PART 2 – PROCESSING DETAILS

1. List of Parties

Data exporter(s): *To be completed by customer:*

- Name:
- Address: [INSERT ADDRESS]
- Contact person's name, position and contact details: [INSERT CONTACT DETAILS]
- Activities relevant to the data transferred under the SCCs: The activities relevant to the personal data transferred under the SCCs are solely as necessary to perform data exporter's obligations under the Agreement.
- Signature and date: see above
- Role (controller/processor) with respect to Shared Personal Data: Controller
- Role (controller/processor) with respect to Customer Personal Data: Controller

Data importer(s):

- Name: Amplify Education, Inc.
- Address: 55 Washington St., Ste 800, Brooklyn, NY 11201
- Contact person's name, position and contact details: Inna Barmash, General Counsel, ibarmash@amplify.com
- Activities relevant to the data transferred under these Clauses: The activities relevant to the personal data transferred under the SCCs are solely as necessary to perform data importer's obligations under the Agreement.
- Signature and date: see above
- Role (controller/processor) with respect to Shared Personal Data: Controller
- Role (controller/processor) with respect to Customer Personal Data: Processor

2. Subject matter of Processing

The subject matter of the Processing of the personal data are set out in the Agreement and this DPA.

3. Duration of Processing

The duration of the Processing activities shall be for the term set forth in the Agreement between Customer and Amplify.

4. Nature and Purpose of Processing

- The Shared Personal Data transferred will be subject to the following basic processing activities: The transfer is made for the purposes identified in clause 3.2 of Part 1 of this DPA.

- The Customer Personal Data transferred will be subject to the following basic processing activities: Transmitting, collecting, storing and analysing data in order to provide the Services to the Customer, and any other activities related to the provision of the Services or specified in the Agreement.

5. Categories of Personal Data

The categories of Shared Personal Data to be Processed:

- *Device information: device type and model, browser configurations and persistent identifiers, such as IP addresses and unique device identifiers.*
- *Diagnostic information: battery level, usage logs and error logs;*
- *Usage information: information about the number of requests a device makes*

The categories of Customer Personal Data to be Processed:

Students:

- *Contact information: name, email address;*
- *Student information: school, grade level, school ID number;*
- *Parent / guardian details: name, email address*
- *Teacher details: name, email address*
- *Schoolwork generated content: information contained in student assignments and assessments, content uploaded by students, responses to questions and participation in activities*
- *Student demographic data: socio-economic status, race, national origin*

Teachers:

- *Contact information: name, phone number, email address;*
- *School information: school, school ID number, approximate location;*
- *Communications: the content of communications or queries submitted to Amplify*

Administrative users of Amplify's service:

- *Contact information: name, phone number, email address;*
- *School information: school, school ID number, approximate location;*
- *Communications: the content of communications or queries submitted to Amplify.*

6. Data Subjects

- Data subjects whose personal data is considered Shared Personal Data and is subject to processing may include: *Users of Amplify's Services, including students, teachers, customer's authorised administrative users*

- Consumers whose personal data is considered Customer Personal Data and is subject to processing may include: *Students, teachers, customer's administrative users (employees and contractors)*

7. **Frequency of transfer**

The Shared Personal Data and Customer Personal Data transferred, including as specified under Modules 1 and 2 above, is transferred on a continuous basis.

8. **Maximum data retention periods, if applicable**

The Shared Personal Data and Customer Personal Data transferred, including as specified under Modules 1 and 2, is retained for so long as is necessary for the relevant Party to perform its obligations under the Agreement or as otherwise necessary for the relevant Party's compliance with its legal and regulatory obligations.

9. **Personal data transferred to and processed by sub-processors**

Subject matter, nature, and duration of Processing Customer Personal Data by sub-processors: see Part 3 Permitted Sub-Processors) below.

Sub-processor Technical and Organisational Measures ("TOMs"): Amplify's sub-processors, in order to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter, shall implement and maintain technical and organisational measures that meet or exceed Amplify's TOMs as set out in Part 4 (Technical and Organisational Security Measures) below.

10. **Supervisory Authority**

To the extent applicable, the competent supervisory authority/ies in accordance with Clause 13 shall be Ireland.

PART 3 – AMPLIFY'S EXISTING SUBPROCESSOR'S

Customer has authorized the use of the following Subprocessors:

See http://www.amplify.com/subprocessors

Part 4 – Technical and Organisational Security Measures

See http://www.amplify.com/security for detailed description of technical and organizational security measures Amplify undertakes to safeguard Personal Data.

Part 5 – UK Addendum

This UK Addendum ("**Addendum**") has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The effective date of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: [INSERT] Trading name (if different): [INSERT] Main address (if a company registered address): see Part 2 above Official registration number (if any) (company number or similar identifier):[INSERT]	Full legal name: Amplify Education, Inc. Trading name (if different): Main address (if a company registered address): see Part 2 above Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): See Part 2 above Job Title: See Part 2 above Contact details including email: See Part 2 above	Full Name (optional): See Part 2 above Job Title: See Part 2 above Contact details including email: See Part 2 above
Signature (if required for the purposes of Section 2)	see above	see above

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:

	Date: The effective date of the Agreement Reference (if any): N/A Other identifier (if any): N/A Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Part 2 above
Annex 1B: Description of Transfer: See Part 2 above
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Section IV.1. of the DPA above
Annex III: List of Sub processors (Modules 2 and 3 only): See Part 3 above

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.