



## DISCOVERY EDUCATION DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules, (“**DPA**”) forms part of the Standard Terms of Service and License (the “**Agreement**”) between Discovery Education Europe Limited and its Affiliates (collectively, “**Discovery Education**”) and the subscriber to the relevant Discovery Education Services (“**Subscriber**”) to reflect the Parties’ agreement with respect to the Processing of Subscriber Data. Discovery Education and Subscriber are each referred to herein as a “**Party**” and collectively as the “**Parties**.”

Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by, and including, this DPA. Except as modified below, the terms of the Agreement shall remain in full force and effect.

### 1. Definitions and Interpretation

1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

“**Affiliates**” means, any person, corporation, company, partnership, joint venture, or other entity controlling, controlled by, or under common control with the applicable Party. For such purpose, the term “**control**” means the holding of 50% or more of the common voting stock or ordinary shares in, or the right to appoint 50% or more of the directors of, the corporation, company, partnership, joint venture, or entity.

“**Account Data**” means Personal Data that relates to Subscriber’s relationship with Discovery Education, including to access Subscriber’s account and billing information, identity verification, maintain or improve performance of the Services, provide support, investigate and prevent system abuse, or fulfill legal obligations.

“**Applicable Data Protection Laws**” means applicable laws relating to privacy and/or data protection, which are applicable to either Party. It shall include without limitation and as applicable (i) the EU e-Privacy Directive 2002/58/EC as implemented by countries within the European Economic Area (“**EEA**”); (ii) the EU General Data Protection Regulation (EU) 2016/679 (“**GDPR**”) as implemented by countries within the EEA; (iii) the UK Data Protection Act 2018, the UK Privacy and Electronic Communications (EC Directive) Regulations 2003, and the GDPR as retained as UK law by the European Union (Withdrawal) Act 2018 (“**UK GDPR**”); (iv) the Swedish Data Protection Act (2018:218); and (v) other laws, rules and regulations that are similar, equivalent to, or successors to the laws that are identified in (i) through (iv) above.

“**Restricted Transfer**” means (a) a transfer of Subscriber Data from or which originated in the EEA to a country outside of the EEA that is not considered to provide an “adequate level” of data protection by the European Commission and where such transfer is subject to the GDPR (“**EEA Restricted Transfer**”) and (b) a transfer of Subscriber Data from or which originated in the UK to a country outside of the UK that is not considered to provide an “adequate level” of data protection by the UK Government and where such transfer is subject to the UK GDPR (“**UK Restricted Transfer**”).

“**Services**” means the services and other activities to be supplied to or carried out by or on behalf of Discovery Education for Subscriber pursuant to the Agreement.

“**Standard Contractual Clauses**” means the Standard Contractual Clauses for the transfer of Personal Data to Third Countries set out in Commission Implementing Decision (EU) 2021/914 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 and available at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=e](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=e).

“**Subscriber Data**” means any Personal Data Processed by Discovery Education in connection with the provision of Services to Subscriber.

“**UK Addendum**” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the Standard Contractual Clauses defined above) issued by the Commissioner under

S119A(1) Data Protection Act 2018, Version B1.0, in force 21 March 2022 and available at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>.

- 1.2 The terms “**Controller**,” “**Data Subject**,” “**Personal Data**,” “**Processor**,” and “**Processing**” have the meanings given to them in Applicable Data Protection Law(s). If and to the extent that Applicable Data Protection Law(s) does not define such terms, then the definitions given in GDPR will apply.
- 1.3 All terms not defined herein will have the same meaning as set forth in the Agreement or the Applicable Data Protection Laws.

## **2. Role and Scope of Processing**

- 2.1 **Scope.** This DPA will apply only to the extent that Discovery Education Processes Subscriber Data, on behalf of Subscriber, to which Applicable Data Protection Laws apply.
- 2.2 **Details of Processing.** The details of Discovery Education’s Processing of Subscriber Data are described in Schedule 1 to this DPA.
- 2.3 **Discovery Education as a Processor.** The parties acknowledge and agree that regarding the Processing of Subscriber Data, Discovery Education is a Processor. Discovery Education will Process Subscriber Data in accordance with Subscriber’s instructions as set forth in Section 3 (Subscriber Instructions).
- 2.4 **Discovery Education as a Controller of Account Data.** The parties acknowledge that, regarding the Processing of Account Data, Subscriber is a controller and Discovery Education is an independent controller, not a joint controller with Subscriber. Discovery Education will Process Account Data as a controller (a) in order to manage the relationship with Subscriber; (b) carry out Discovery Education’s core business operations; (c) in order to detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) identity verification; (e) to comply with Discovery Education’s legal or regulatory obligations; and (f) as otherwise permitted under Applicable Data Protection Laws and in accordance with the Agreement.

## **3. Processing of Subscriber Data**

- 3.1 **Subscriber Instructions.** Subscriber appoints Discovery Education as a Processor to Process Subscriber Data on behalf of, and in accordance with, Subscriber’s instructions (a) as set forth in the Agreement and as otherwise necessary to provide the Services to Subscriber (which may include investigating security incidents, and detecting and preventing exploits or abuse); (b) as necessary to comply with applicable legal or regulatory obligations, including Applicable Data Protection Laws; and (c) as otherwise agreed in writing between the parties.
- 3.2 **Lawfulness of Instructions.** Subscriber will ensure that its instructions comply with Applicable Data Protection Laws. Subscriber acknowledges that Discovery Education is neither responsible for determining which laws or regulations are applicable to Subscriber’s business nor whether Discovery Education’s provision of the Services meets or will meet the requirements of such laws or regulations. Subscriber will ensure that Discovery Education’s Processing of Subscriber Data, when done in accordance with Subscriber’s instructions, will not cause Discovery Education to violate any applicable law or regulation, including Applicable Data Protection Laws. Discovery Education will inform Subscriber if it becomes aware, or reasonably believes, that Subscriber’s instructions violate any applicable law or regulation, including Applicable Data Protection Laws.
- 3.3 Subscriber shall, in its use of the Services, Process Personal Data in accordance with the requirements of Applicable Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of Discovery Education as Processor.
- 3.4 Discovery Education shall:
  - 3.4.1 comply with Applicable Data Protection Laws in the Processing of Subscriber Data;
  - 3.4.2 use Subscriber Data only for the purpose of fulfilling its respective duties and providing the Services under the Agreement; and

3.4.3 not otherwise Process Subscriber Data other than on Subscriber's documented instructions unless Processing is required by Applicable Data Protection Laws to which Discovery Education is subject, in which case Discovery Education shall to the extent permitted by Applicable Data Protection Laws inform Subscriber of that legal requirement before the relevant Processing of that Subscriber Data.

3.5 Subscriber instructs Discovery Education (and authorizes Discovery Education to instruct each Sub-processor) to Process Subscriber Data; and in particular, transfer Subscriber Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Agreement.

#### 4. **Discovery Education Personnel**

4.1 **Confidentiality.** Discovery Education shall ensure that its personnel engaged in the Processing of Subscriber Data are informed of the confidential nature of Subscriber Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements.

4.2 **Reliability.** Discovery Education shall take commercially reasonable steps to ensure the reliability of its personnel engaged in Processing Subscriber Data.

#### 5. **Security**

5.1 Discovery Education shall maintain appropriate technical and organizational measures to protect Subscriber Data. Subscriber acknowledges that the technical and organizational measures are subject to technical progress and development and that Discovery Education may update or modify the technical and organizational measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services.

#### 6. **Sub-processors**

6.1 **Appointment of Sub-processors.** Subscriber acknowledges and agrees that Discovery Education's Affiliates may be retained as Sub-processors, and Discovery Education and its Affiliates may engage Sub-processors in connection with the provision of the Services.

6.2 **Sub-processor List.** Discovery Education's current list of Sub-processors engaged in Processing Personal Data for the performance of the Services is available on Discovery Education's Sub-processor webpage available at <https://www.discoveryeducation.co.uk/subprocessor/>. Subscriber consents to Discovery Education's use of these Sub-processors.

6.3 **Notice.** Discovery Education will give Subscriber prior written notice of the appointment of any new Sub-processor. Subscriber may object to Discovery Education's appointment of any new Sub-processor in writing by email to [ukprivacy@discoveryed.com](mailto:ukprivacy@discoveryed.com) within 10 business days of receipt of notice if Subscriber has reasonable concerns related to such Sub-processor's ability to comply with Applicable Data Protection Laws. Upon Subscriber's objection, the parties shall work together in good faith to address Subscriber's concerns. If the parties are unable to reach a resolution, Subscriber may terminate the applicable Order Form(s) with respect to only those Services that cannot be provided by Discovery Education without the use of the objected-to new Sub-processor by providing written notice to Discovery Education. In such case, Discovery Education will refund Subscriber a pro-rated amount to reflect any prepaid fees that cover the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services.

6.4 Discovery Education will enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect Subscriber Data to the standard required by Applicable Data Protection Laws.

#### 7. **Data Subject Rights**

Taking into account the nature of the Processing, Discovery Education will provide reasonable and timely assistance (at Subscriber's expense) to enable Subscriber to respond to any request from a Data Subject to exercise any of its rights under Applicable Data Protection Laws. Discovery Education shall notify Subscriber about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed or required to do so in order to comply with applicable laws).

## **8. Government Access Requests**

If Discovery Education receives a legally binding request to access Subscriber Data from a law enforcement authority or regulator, Discovery Education shall, unless otherwise legally prohibited, give reasonable notice to Subscriber, including a summary of the nature of the request, to allow Subscriber to seek a protective order or other appropriate remedy. To the extent Discovery Education is prohibited by law from providing such notification, Discovery Education shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Discovery Education to communicate as much information as possible, as soon as possible. Discovery Education will attempt to redirect the law enforcement agency or regulator to request that data directly from Subscriber. As part of this effort, Discovery Education may provide Subscriber's contact information to the law enforcement agency or regulator. Discovery Education shall not disclose the Subscriber Data requested until required to do so under the applicable procedural rules. Discovery Education agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. Discovery Education shall promptly notify Subscriber if Discovery Education becomes aware of any direct access by a law enforcement authority or regulator to Subscriber Data and provide information available to Discovery Education in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require Discovery Education to pursue action or inaction that could result in civil or criminal penalty for Discovery Education such as contempt of court.

## **9. Personal Data Breach**

9.1 Discovery Education shall notify Subscriber without undue delay upon Discovery Education becoming aware of a Personal Data Breach affecting Subscriber Data.

9.2 In the event of a Personal Data Breach, Discovery Education is not authorized to notify a data protection or other authority, the Data Subjects concerned, or any other third parties unless Discovery Education is required to do so under Applicable Data Protection Laws. In such event, Discovery Education shall, to the extent permitted under Applicable Data Protection Laws, liaise and coordinate with Subscriber prior to making a notification.

## **10. Data Protection Impact Assessment and Prior Consultation**

Discovery Education shall provide reasonable assistance to Subscriber with any data protection impact assessments and prior consultations with supervisory authorities or other regulatory entities which Subscriber reasonably considers to be required of Subscriber by any Applicable Data Protection Laws, in each case solely in relation to Processing of Subscriber Data by, and taking into account the nature of the Processing and information available to, Discovery Education.

## **11. Deletion or Return of Subscriber Data**

At the choice of Subscriber, Discovery Education will delete or return all Subscriber Data (including copies) Processed on behalf of Subscriber; provided that Discovery Education may anonymize Subscriber Data so that it is no longer personally identifiable and may retain the resulting anonymized data. This requirement does not apply to the extent Discovery Education is required by applicable law to retain some or all of the Subscriber Data, or to Subscriber Data it has archived on back-up systems, which Subscriber Data Discovery Education will securely isolate and protect from any further Processing.

## **12. Audit**

12.1 Subject to subsections 12.2 to 12.4, upon request, Discovery Education will make available to Subscriber all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Subscriber or an auditor mandated by Subscriber in relation to the Processing of the Subscriber Data by Discovery Education. Any audit performed pursuant to this Section will be conducted under a non-disclosure agreement and any information or report derived from such audit will be deemed Discovery Education's Confidential Information. Subscriber cannot exercise this right more than once per calendar year.

12.2 Upon Subscriber's request to perform an inspection or audit in accordance with subsection 12.1, to the extent permitted by the Applicable Data Protection Laws, Discovery Education may elect to retain a qualified and independent assessor to perform such inspection or audit, using an appropriate and accepted

control standard or framework and assessment procedure for such assessments. On the condition that Subscriber has entered into an applicable non-disclosure agreement with Discovery Education, Discovery Education may supply (on a confidential basis) a summary copy of its audit report to Subscriber; and provide written responses (on a confidential basis) to all reasonable requests for information made by Subscriber related to its Processing of Subscriber Data, including responses to information security and audit questionnaires, that are necessary to confirm Discovery Education's compliance with this DPA.

12.3 Subscriber will give Discovery Education reasonable notice of any audit or inspection to be conducted under subsection 12.1 and shall make (and ensure that each of its mandated auditors makes) reasonable efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to Discovery Education's and/or any Sub-processor's premises, equipment, personnel, and business while its personnel are on those premises in the course of such an audit or inspection. Discovery Education and any Sub-processor(s) need not give access to its premises for the purposes of such an audit or inspection:

12.3.1 to any individual unless they produce reasonable evidence of identity and authority;

12.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Subscriber has given notice to Discovery Education that this is the case before attendance outside those hours begins; or

12.3.3 for the purposes of more than one audit or inspection of Discovery Education or any Sub-processor in any calendar year, except for any additional audits or inspections which:

12.3.3.1 Subscriber reasonably considers necessary because of genuine concerns as to Discovery Education's compliance with this DPA; or

12.3.3.2 Subscriber is required or requested to carry out by the Applicable Data Protection Laws, a Supervisory Authority, or any similar regulatory authority responsible for the enforcement of the Applicable Data Protection Laws in any country or territory,

where Subscriber has identified its concerns or the relevant requirement or request in its notice to Discovery Education of the audit or inspection.

12.4 Each party shall bear its own costs with respect to any audit and/or inspection.

### 13. Transfer Mechanisms for Restricted Transfers

13.1 **EEA Restricted Transfers.** The Parties acknowledge and agree that to the extent a Party undertakes an EEA Restricted Transfer, the Parties shall Process Subscriber Data which is subject to the EEA Restricted Transfer in accordance with the Standard Contractual Clauses, appended hereto as Schedule 2.

13.2 **UK Restricted Transfers.** The Parties acknowledge and agree that to the extent a Party undertakes a UK Restricted Transfer, the parties shall Process Subscriber Data which is subject to the UK Restricted Transfer in accordance with the UK Addendum, appended hereto as Schedule 3.

13.3 **Modules Applicable.** The Parties acknowledge and agree that:

13.3.1 **Module 1.** Where either Party and/or its Authorized Affiliate (acting as a controller) undertakes a Restricted Transfer to the other Party (also acting as a controller), then the Parties shall comply with Module 1 of the Standard Contractual Clauses.

13.3.2 **Module 2.** Where Subscriber and/or its Authorized Affiliate is a Controller and a data exporter, and Discovery Education is a Processor and data importer in respect of that Subscriber Data, then the Parties shall comply with Module 2 of the Standard Contractual Clauses.

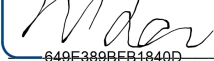
## 14. General Terms

- 14.1 **Governing law and jurisdiction.** This DPA is governed by the laws of the jurisdiction agreed to by the Parties as governing the Agreement. Notwithstanding the foregoing, the provisions set out in the Standard Contractual Clauses and the UK Addendum shall be governed by, and subject to the jurisdiction of, the relevant law and courts as set forth in the Standard Contractual Clauses and the UK Addendum as applicable. This DPA is in addition to the rights related to privacy or data security set forth in the Agreement.
- 14.2 **Order of precedence.** To the extent: (i) the terms contained in this DPA conflict with those contained in the Agreement, the terms in this DPA shall govern and control to the extent such conflict relates to the Processing of Subscriber Data; and (ii) the terms contained in the UK Addendum conflict with those in the Standard Contractual Clauses, the terms in the UK Addendum shall prevail in accordance with the Hierarchy provisions therein to the extent the conflict relates to a UK Restricted Transfer.
- 14.3 Obligations of confidentiality of Subscriber Data Processed pursuant to this DPA shall survive termination of the Agreement.
- 14.4 Except to the extent set out in subsection 14.5, it is the express intent of the Parties that any person who is not a party to this DPA has no right, as third party beneficiary, under local legal principle or law, to enforce any term of this DPA, and accordingly nothing contained in this DPA will entitle any person (including, data subjects) other than the parties to this DPA, to any claim, cause of action, remedy or right of any kind whatsoever.
- 14.5 The Parties agree that a data subject may enforce the terms of the Standard Contractual Clauses and the UK Addendum (as applicable) as provided therein.
- 14.6 **Amendment.** This DPA may only be amended by a specific amendment to this DPA signed by both Parties hereto. Notwithstanding the foregoing, the Parties acknowledge that should the European Commission, or UK Government publish new standard contractual clauses or similar (or amendments to the existing Standard Contractual Clauses and/or UK Addendum) to address Restricted Transfers, and where the Parties determine such new or amended clauses are required to address the Restricted Transfers, such new or amended clauses will replace the Standard Contractual Clauses and/or UK Addendum attached to this DPA upon either Party's notification to other Party thereof. All Restricted Transfers will be thereafter made pursuant to such new or amended clauses.
- 14.7 **Indemnification.** Each of the parties ("**Indemnifying Party**") agrees to indemnify and hold harmless the other party and its officers, employees, directors, and agents ("**Indemnified Party**") from, and at the Indemnifying Party's option defend against, any and all third-party claims, losses, liabilities, damages, costs, and expenses (including attorneys' fees, consultants' fees, and court costs) (collectively, "**Claims**") arising out of the Indemnifying Party's (i) violation of an Applicable Data Protection Law; or (ii) breach of any provision of this DPA.
- 14.8 **Term.** This DPA, including the Standard Contractual Clauses and the UK Addendum (where applicable), will terminate simultaneously and automatically upon deletion by Discovery Education of Subscriber Data Processed on behalf of Subscriber, in accordance with Section 11 of this DPA.
- 14.9 **Changes.** Discovery Education reserves the right to change the terms of this DPA from time to time. Such changes will become effective when Discovery Education posts the revised DPA on the Discovery Education website. Subscriber and Users should check the DPA from time to time, as they are bound by the DPA posted on Discovery Education's website at the time of access. The Parties agree that this DPA replaces and supersedes any existing DPA the parties may have previously entered into in connection with the Services. The current DPA is available at <https://www.discoveryeducation.co.uk/data-processing-addendum/>.
- 14.10 Failure by any Party to enforce any of its rights under this DPA shall not be taken as or deemed to be a waiver of such right.
- 14.11 If any part, term or provision under this DPA is held to be illegal or unenforceable, the validity or enforceability of the remainder of this DPA will not be affected.

14.12 Execution of this DPA by either Party shall be deemed acceptance and execution by that Party of the Schedules, which are duly incorporated into this DPA.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement.

**Discovery Education**



649E389BFB1840D...

Signature

Howard Lewis

Name

Managing Director

Title

May 9, 2023

Date

**Subscriber**

Signature

Name

Title

Date

## Schedule 1

### Description of Processing/Transfer

#### 1. List of Parties

##### Data exporter(s):

**Name:** The entity identified as Subscriber in the applicable Order Form.

**Address:** The address for the Subscriber associated with its Discovery Education account.

**Contact person's name, position and contact details:** The contact details for the Subscriber associated with its Discovery Education account.

**Activities relevant to the data transferred under these Clauses:** The transfer of Subscriber Data from data exporter to data importer in the context of the Agreement.

**Signature and date:** *Execution of the DPA on the Effective Date is deemed execution of these Clauses which are incorporated therein.*

**Role (controller/processor):** For the purposes of Module 2, Subscriber is a Controller.

##### Data importer(s):

**Name:** Discovery Education Europe Limited

**Address:** 9 Palace Yard Mews, Bath BA1 2NH United Kingdom

**Contact person's name, position and contact details:** Legal Department [ukprivacy@discoveryed.com](mailto:ukprivacy@discoveryed.com)

**Activities relevant to the data transferred under these Clauses:** Discovery Education is a provider of digital educational services which Processes and transfers Subscriber Data at the instructions of the data exporter in accordance with the terms of the Agreement.

**Signature and date:** *Execution of the DPA on the Effective Date is deemed execution of these Clauses which are incorporated therein.*

**Role (controller/processor):** For the purposes of Module 2, Discovery Education is a Processor.

#### 2. Description of Processing/Transfer

##### *Categories of data subjects whose personal data is transferred*

- Employees, contractors, and agents of Subscriber
- Subscriber's users authorized by Subscriber to use the Services (including administrators, educators, pupils)
- Parents or legal guardians of pupils

##### *Categories of personal data transferred*

- *Employees, contractors, and agents of Subscriber:* first name, last name, business contact information (local authority, school, school address, job title, phone number and email address)
- *Subscriber's users authorized by Subscriber to use the Services (Pupils) (where applicable):* first name, middle initial, last name, username (logon ID), password, month and year of birth (DoodleLearning pupil users only), contact information (email address), ID data (pupil ID, class ID), school, pupil key stage and class, product usage data, device and connection data, including, but not limited to, IP addresses,



persistent identifiers, log files, browsing history, search history, and information regarding interaction with the Discovery Education Services.

- *Subscriber's users authorized by Subscriber to use the Services (Administrators and Educators) (where applicable):* first name, middle initial, last name, username (logon ID), password, month and year of birth (Doodle Learning pupil users only), contact information (school, district, email address, business address, school postcode), ID data (teacher ID, class ID), teacher trade association membership number (such as NAHT membership number), if relevant for a special offer, teacher key stage and class(es), product usage data, device and connection data, including, but not limited to, IP addresses, persistent identifiers, log files, browsing history, search history, and information regarding interaction with the Discovery Education Services
- *Parents or legal guardians of pupils (where applicable):* first name, last name, username (logon ID), password, contact information (email address, phone number, and optionally home address, where physical resources are required to be distributed or to process payment information), product usage data, device and connection data, including, but not limited to, IP addresses, persistent identifiers, log files, browsing history, search history, and information regarding interaction with a website or the Discovery Education Services

***Sensitive data transferred (if applicable)***

Except in the limited circumstances where teachers may be asked to provide their National Association of Head Teachers trade union membership number to receive a discount for certain Services, Subscriber may not submit special categories of Personal Data to the Services.

***The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)***

Continuous

***Nature of the processing***

Subscriber Data will be subject to automated and manual Processing operations by the data importer as necessary to perform the Services under the Agreement.

***Purpose(s) of the data transfer and further processing***

To perform Services under the Agreement.

***The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period***

Discovery Education may retain Subscriber Data for the purposes described above for the duration of the DPA, and for as long as Discovery Education has a legitimate need to retain the Subscriber Data for the purposes for which it was collected or transferred, in accordance with Applicable Data Protection Laws.

***For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing***

For the subject matter, nature and duration as identified above.

**3. Competent Supervisory Authority**

The supervisory authority of the EEA country where (i) the data exporter is established; or where (ii) the EU representative of the data exporter is established.

**4. Technical and Organisational Security Measures**

Discovery Education maintains appropriate technical and organisational security measures for protection of the security, confidentiality and integrity of Subscriber Data, as described in the IT Security Policies applicable to the specific Services purchased by Subscriber, and set forth in Annex II attached hereto.

**Schedule 2**

**Standard Contractual Clauses  
(European Commission Implementing Decision (EU) 2021/914 4 June 2021)**

**SECTION 1**

*Clause 1*

***Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3*

***Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

- (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 – Module One: Clause 12(a) and (d); Module Two: Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 – Modules One and Two: Clause 18(a) and (b)
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU)2016/679.
- (c)

*Clause 4*

***Interpretation***

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*

***Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7 – Optional*

***Docking clause***

*Deliberately omitted.*

**SECTION 2 - OBLIGATIONS OF THE PARTIES**

*Clause 8*

***Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

## **MODULE ONE: Transfer controller to controller**

### **8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- (a) where it has obtained the data subject's prior consent;
- (b) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (c) where necessary in order to protect the vital interests of the data subject or of another natural person.

### **8.2 Transparency**

- (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
  - (i) of its identity and contact details;
  - (ii) of the categories of personal data processed;
  - (iii) of the right to obtain a copy of these Clauses;
  - (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- (b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (c) On request, the Parties shall make a copy of these Clauses, including the Appendixes completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### **8.3 Accuracy and data minimisation**

- (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

#### 8.4 **Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

#### 8.5 **Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

#### 8.6 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter “sensitive data”), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data,

additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

#### 8.7 **Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (a) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- (c) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (d) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (e) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (f) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### 8.8 **Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

#### 8.9 **Documentation and compliance**

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

### **MODULE TWO: Transfer controller to processor**

#### 8.1 **Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

## 8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

## 8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

## 8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

## 8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

## 8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to

mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

#### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

#### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### 8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.



- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Clause 8*

***Use of sub-processors***

**MODULE TWO: Transfer controller to processor**

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 9*

***Data subject rights***

**MODULE ONE: Transfer controller to controller**

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- (b) In particular, upon request by the data subject the data importer shall, free of charge:
  - (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of

such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

- (ii) rectify inaccurate or incomplete data concerning the data subject;
  - (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lay down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
- (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
  - (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- (g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

## **MODULE TWO: Transfer controller to processor**

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

### *Clause 10*

#### ***Redress***

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (i) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.
- (a) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (b) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (c) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (d) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (e) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 11*

***Liability***

**MODULE ONE: Transfer controller to controller**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

**MODULE TWO: Transfer controller to processor**

- (b) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (c) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (d) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (e) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (f) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (g) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (h) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 12*

*Supervision*

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

- (a) **Where the data exporter is established in an EU Member State:** The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

**Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:** The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

**Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with Article 3(2) without**

**however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:**

The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

*Clause 13*

*Local laws and practices affecting compliance with the Clauses*

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

#### *Clause 14*

#### ***Obligations of the data importer in case of access by public authorities***

#### **MODULE ONE: Transfer controller to controller**

#### **MODULE TWO: Transfer controller to processor**

##### **14.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

##### **14.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable

procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **SECTION IV – FINAL PROVISIONS**

##### *Clause 15*

##### ***Non-compliance with the Clauses and termination***

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) **For Modules One and Two:** Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

##### *Clause 16*

##### ***Governing law***

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

*Clause 17*

***Choice of forum and jurisdiction***

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.



## Annexes I – III to the EU Standard Contractual Clauses (Schedule 2)

### Annex I

The details of data transfers are set out in Schedule 1 of the DPA.

### Annex II – Technical and Organisational Measures

**Purpose.** This Annex II describes Discovery Education’s security program, and physical, technical, organizational, and administrative controls and measures to protect Subscriber Data from unauthorized access, destruction, use, modification, or disclosure (the “**Security Measures**”). Unless otherwise specified, the Security Measures apply to Discovery Education Experience, Espresso, Coding, Health & Relationships, STEM Connect, and DoodleLearning.

**Definitions.** Any capitalized terms used but not defined in this document have the meanings set out in the Agreement or DPA.

Discovery Education has implemented the following Security Measures:

1. **Organizational Measures.**
  - a. Discovery Education has a designated security officer responsible for overseeing its security program.
  - b. Information security personnel are trained and qualified.
  - c. Information security training and awareness is conducted and provided to Discovery Education employees.
2. **Access and Management Controls.** Discovery Education implements procedures designed to limit personnel’s access to Subscriber Data as follows:
  - a. Limits internal access to Subscriber Data, applications, and systems to Discovery Education personnel with proper authorization and allow use and/or disclosure internally, when necessary, solely to personnel based on legitimate business need.
  - b. Revokes access to personnel who no longer require access.
  - c. Requires use of strong passwords or pass phrases.
  - d. Logically separates Subscriber Data and maintains measures designed to prevent Subscriber Data from access by other users.
  - e. Restricts access to Discovery Education proprietary source code to prevent unauthorized access.
3. **Network Security, Physical Security and Environmental Controls.** Discovery Education implements network security, physical security and environmental controls as follows:
  - a. Network intrusion detection and network intrusion prevention technology.
  - b. Physical access controls to processing premises and facilities, provisioning access to the processing facilities on the basis of the role (need to know), and utilizing physical Access Control Mechanisms such as Electronic Access Control (EAC) cards to access server rooms, install CCTV systems, etc.
  - c. For remote access connections, requires multifactor authentication and the use of a VPN connection for certain personnel to certain systems and applications.
  - d. Properly configured and patched firewalls, network access controls and other technical measures designed to prevent unauthorized access to systems processing Subscriber Data.
  - e. Perform routine maintenance to ensure operating systems and applications are patched and updated.

- f. Monitors security release information for software. Discovery Education prioritizes the rollout of patches based on the severity or impact of the vulnerability.
  - g. Process for monitoring, alerting, and responding to suspicious activity occurring in the Discovery Education infrastructure.
  - h. Discovery Education Services operate on Amazon Web Services (AWS) and is protected by Amazon's security and environmental controls.
  - i. Subscriber Data hosted in AWS is encrypted at rest and in transit. AWS does not have access to unencrypted Subscriber Data.
4. **Operating System Security.** Discovery Education implements operating security controls as follows:
- a. Operating systems are protected with anti-malware/virus protection software.
  - b. Server and cloud operating systems are deployed using a secure build process.
  - c. Security logging is enabled per vendor recommendations for all desktop, server, and network infrastructure OS.
  - d. Supported operating system versions.
  - e. Anti-virus signatures are updated regularly.
5. **Data Encryption and Pseudonymisation.** Discovery Education implements data encryption and pseudonymization as follows:
- a. Implements encryption in transport and at rest.
  - b. Implements pseudonymization of Subscriber Data, where appropriate.
  - c. Uses industry standard encryption methodologies to protect Subscriber Data.
  - d. Implements full-disk encryption for hard-drives on personnel workstations.
  - e. External data transmissions of Subscriber Data are encrypted using industry standard security protocols.
6. **Incident Response.**
- a. Discovery Education maintains an information security incident response plan that is tested at least annually.
  - b. Discovery Education implements and maintains technology designed to detect suspicious activity, malicious activity, vulnerabilities and security incidents within Discovery Education's network and systems.
7. **Vulnerability Management.** Discovery Education maintains the following vulnerability management processes for devices used to connect to the Discovery Education network:
- a. Discovery Education will employ industry standards and tools to conduct routine infrastructure vulnerability scanning to test Discovery Education's network and application penetration testing of the Discovery Education Services. The results are triaged by the information security team.
  - b. Discovery Education has processes in place designed to ensure adherence to industry standard security development practices for development and testing for code, APIs, and applications deployed and implemented in support of the Discovery Education Services.
8. **Monitoring and Logging.**
- a. Discovery Education has implemented procedures to log and regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.
  - b. Discovery uses a variety of approaches and technologies to make sure that risks and incidents are appropriately detected, assessed and mitigated on an ongoing basis.

**9. Business Continuity Management.**

- a. Discovery Education maintains a business continuity and disaster recovery plan.
- b. Discovery Education maintains processes to ensure failover redundancy with its systems, networks and data storage.

**10. Personnel Management.**

- a. For U.S. Discovery Education employees, Discovery Education performs employment verification, including proof of identity validation, check of education records and employment track, and criminal background checks for new hires in positions requiring access to systems and applications storing Subscriber Data in accordance with applicable law. For non-U.S. Discovery Education employees, Discovery Education will use commercially reasonable efforts to meet the same criteria as established for U.S.-based Discovery Education employees, subject to general business practices in the respective country and in compliance with applicable local law requirements.
- b. Upon employee termination, whether voluntary or involuntary, Discovery Education immediately disables all access to Discovery Education systems and physical facilities.

**Updates and Modifications.** The Security Measures are subject to technical progress and development. Discovery Education may update or modify the Security Measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services.

**Annex III – List of Sub-processors**

Discovery Education's current list of Sub-processors can be found at <https://www.discoveryeducation.co.uk/subprocessor/>.

**Schedule 3****International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the “Addendum”) (Version B1.0, in force 21 March 2022)****Part 1: Tables**

<b>Start date</b>	Effective Date of the DPA	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties’ details</b>	See Schedule 2, Annex 1(1), of the DPA	See Schedule 2, Annex 1(1), of the DPA
<b>Key Contact</b>	See Schedule 2, Annex 1(1), of the DPA	See Schedule 2, Annex 1(1), of the DPA
<b>Signature (if required for the purposes of Section 2)</b>	Execution of the DPA on the Effective Date is deemed execution of this Addendum	Execution of the DPA on the Effective Date is deemed execution of this Addendum

**Table 2: Selected SCCs, Modules and Selected Clauses**

<b>Addendum EU SCCs</b>	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective Date of DPA Reference (if any): None Other identifier (if any): None
-------------------------	---

**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 1(1) – (3) A: List of Parties: See Schedule 2, Annex 1, of the DPA

Annex 1(1) – (3) B: Description of Transfer: See Schedule 2, Annex 1, of the DPA

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule 2, Annex II, of the DPA

Annex III: List of Sub-processors (Module 2 only): See Schedule 2, Annex III, of the DPA

**Table 4: Ending this Addendum when the Approved Addendum Changes**

<b>Ending this Addendum when the Approved Addendum changes</b>	Which Parties may end this Addendum as set out in Section 19: <input type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party
--	--

**PART 2: MANDATORY CLAUSES**

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 of 2019 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.