DISCOVERY EDUCATION DATA PROTECTION ADDENDUM

This Discovery Education Student Data Protection Addendum ("**DPA**") forms part of the Standard Terms of Service and License (the "**Standard Terms**") and describes Discovery's obligations to protect Personal Data (defined below) during Discovery's provision of the Services to Subscriber. Capitalized terms not otherwise defined in this DPA shall have the meanings ascribed to them in the Standard Terms.

1. **Personal Data and Purpose of DPA**. This DPA serves to comply with Data Protection Laws (defined below). As between Subscriber and Discovery, Subscriber or the party who provided such data (such as the student or parent or educator), is the exclusive owner of all right, title, and interest in and to any and all Personal Data disclosed or transmitted to Discovery under the Agreement and this DPA. Discovery hereby waives any and all statutory and common law liens it may now or hereafter have with respect to Subscriber's Personal Data. Nothing in the Agreement or this DPA will operate as an obstacle to Subscriber's right to retrieve any and all Personal Data disclosed or transmitted to Discovery under the Agreement and this DPA. Subscriber and Discovery acknowledge and agree that to the extent Data Protection Laws apply to the Processing of Personal Data under the Agreement, Subscriber is the Controller and Discovery is the Processor. The Parties acknowledge and agree that as with respect to authorized user data of the parents and educators, Discovery is the Controller and will process the information for all Dreambox Learning products in accordance with the Privacy policy located here: https://www.dreambox.com/privacy-policy and for all other products in accordance with its privacy policy located here: https://www.discoveryeducation.com/privacy-policy/. For the avoidance of doubt, this DPA does not relieve either Party from the liability imposed on it under Data Protection Laws by virtue of its role in the Agreement and this DPA.

2. **Consents and Notifications for Disclosures of Personal Data**. The Parties acknowledge and agree that Discovery meets the requirements contained in 34 CFR § 99.31(a) and qualifies as a school official pursuant to FERPA (defined below). Notwithstanding the foregoing, Subscriber affirms, represents, and warrants that it has obtained, and is solely responsible for: (i) the accuracy and quality of Personal Data; and (ii) obtaining, all consents as may be required by Data Protection Laws, as well as making all required disclosures to the individuals, parents, legal guardians, and students as may be required by Data Protection Laws, to disclose or transmit Personal Data to Discovery. Subscriber will provide proof of the required consent within five (5) business days of Discovery's written request. Subscriber will notify Discovery concerning any changes to its public school district or its administrators, faculty members, staff members, students, parents, or guardians that may affect Discovery's compliance with this DPA.

3. **Discovery Processing of Personal Data**.

3.1 Discovery will only Process Personal Data on behalf of Subscriber for Business Purposes, unless required to do so by applicable Law (defined below), in which case Discovery will, without undue delay, notify Subscriber of such requirement. The instructions set forth in this DPA, the Standard Terms, any Order Form, or other duly documented instructions are Subscriber's complete instructions to Discovery for the Processing of Personal Data. The Parties acknowledge and agree that Subscriber is disclosing Personal Data to Discovery only for Business Purposes. Notwithstanding the foregoing, Subscriber authorizes Discovery to use Personal Data internally, including for assessing, improving, and developing its Services, business, and for other analytics, marketing, and research purposes, provided that Discovery does not share the Personal Data in identified format.

3.2 Discovery will notify Subscriber, without undue delay, but within no more than five (5) days, if it determines that it is no longer able to comply with its obligations under Data Protection Laws.

3.3 Other than as set forth in Section 9, Discovery will not: (i) retain, use, or disclose Personal Data for any purpose, including, without limitation, any commercial purpose other than Business Purposes, unless expressly permitted by Data Protection Laws or permitted in this Section; (ii) Sell or Share Personal Data; (iii) retain, use, or disclose Personal Data for any purpose outside of the Parties' direct business relationship, unless expressly permitted by Data Protection Laws; or (iv) combine or update Personal Data with personal data collected from its own interaction with an individual or received from another source, unless expressly permitted by Data Protection Laws. For the avoidance of doubt, Discovery will not use Personal Data to advertise or market to students or their parents nor will it share Personal Data for purposes of targeted advertising.

4. **Data Security**. In Processing the Personal Data, Discovery will provide at least the same level of privacy protection as required by Data Protection Laws. Discovery represents and warrants that it has implemented and maintains appropriate administrative, physical, and technical measures to ensure a level of security commensurate to the risk to Personal Data and guard against the unauthorized or accidental access, disclosure, destruction, loss, Processing, damage, or alteration of Personal Data, which, are as set forth in the Security Policy in Schedule 1. Subscriber represents and warrants that it has evaluated the

administrative, physical, and technical measures implemented by Discovery as providing an appropriate level of protection for the Personal Data, taking into account the risk associated with the Processing of such information.

5. **Discovery's Personnel and Subcontractors**. Discovery will ensure that its personnel and Subcontractors (defined below) that access the Personal Data are informed of the confidential nature of the Personal Data and are bound by appropriate obligations of confidentiality or are under an appropriate statutory obligation of confidentiality. Discovery will take all reasonable steps and to ensure the reliability of Discovery personnel and Subcontractors that access Personal Data.

6. **Personal Data Requests**. Discovery will, without undue delay, notify, then record, and then refer to Subscriber full details of all Personal Data Requests. In the event Discovery receives a request directly from a student, parent, or guardian, Discovery shall direct such person to submit the request directly to Subscriber. To the extent Subscriber is unable to respond to a Personal Data Request with information available through Discovery's products or services, Discovery will provide reasonable assistance to Subscriber in responding to a Personal Data Request. Discovery will not respond to a Personal Data Request without Subscriber's explicit instruction; provided, however, if required to respond under Laws to which Discovery is subject, Discovery will, to the extent permitted by such Laws, inform Subscriber, by not later than twenty-four (24) hours from receipt of the request, of that legal requirement before it responds to the request.

7. **Personal Data Disclosures**. To the extent legally permissible, Discovery will promptly notify Subscriber of any legally binding request for disclosure or seizure of Personal Data by a government agency or law enforcement authority.

8. **Destruction of Data**. Upon expiration or termination of the Agreement, Discovery will Destroy (defined below) all Personal Data previously received from Subscriber no later than sixty (60) days following such termination, unless a reasonable written request is submitted by Subscriber to Discovery to hold such Personal Data. Discovery may retain Personal Data to the extent required by Laws to which Discovery is subject, or if Personal Data resides in Discovery's backup archives, Discovery will continue to protect the security and confidentiality of such retained Personal Data in accordance with the Agreement and this DPA.

9. **De-identified Data**.

9.1 Discovery may de-identify and aggregate Subscriber's Personal Data with Discovery's other Subscribers' Personal Data and use the de-identified and aggregate data for any lawful purpose, including but not limited to, assessing, improving, and developing its Services, business, and for other analytics, marketing, and research purposes.

9.2 To the extent Discovery collects on behalf of Subscriber or receives from Subscriber de-identified data or pseudonymized data (as those terms are defined under applicable Data Protection Laws) (collectively, "**D&P Data**") or in connection with Discovery's authorized use of D&P Data (as set forth in Section 9.1), Discovery shall implement such deidentification or pseudonymization in accordance with Data Protection Laws. In addition, for de-identified data, Discovery will: (i) take reasonable measures to ensure that the information cannot be, linked, attributed, or otherwise associated with a consumer, household, or device (including without limitation: (a) implement and maintain technical and administrative safeguards that prohibit reidentification of the de-identified data; (b) implement and maintain business processes that specifically prohibit reidentification of the de-identified data and prevent inadvertent release of the de-identified data; and (c) periodically reassess technical safeguards and processes to ensure that they are still adequate to prevent reidentification of and prohibit inadvertent release of the de-identified data); (ii) publicly commit to maintain and use the de-identified data in deidentified form and not to attempt to reidentify the de-identified data; and (iii) contractually obligate any recipients of the de-identified data to comply with all provisions of this Section 9.2.

10. **Personal Data Breach**.

10.1. **Personal Data Breach Notification**. In the event of any Personal Data Breach, upon Discovery becoming aware of such Personal Data Breach, without undue delay Discovery will:

10.1.1. notify Subscriber of the Personal Data Breach; and

10.1.2. provide Subscriber with details that are available to Discovery at the time of notice regarding:

(a) the nature of the Personal Data Breach, including the categories and approximate numbers of students and Personal Data records concerned;

(b) any investigations into such Personal Data Breach; and

(c) any measures taken to address the Personal Data Breach, including to mitigate its possible adverse effects and prevent the re-occurrence of the Personal Data Breach.

10.2. **Notification Sharing**. Subscriber may share any notification and details provided by Discovery under this Section 10 with the appropriate government agency or law enforcement authority if required to do so under the Data Protection Laws.

11. Sub-processing.

11.1 Subscriber hereby approves the Subcontractors currently engaged by Discovery and that are listed in Schedule 2, Schedule 3, Schedule 4, and Schedule 5.

11.2 Discovery will provide written notice to Subscriber within thirty (30) days of engaging a new Subcontractor, and Subscriber will have thirty (30) days to provide written notice of its objection to such Subcontractor. Upon Subscriber's objection in accordance with this Section 11, Discovery will use reasonable efforts to change the provision of the Services in a manner that avoids the use of the proposed Subcontractor. Where such a change cannot be made, notwithstanding anything in the Agreement, Subscriber may, by written notice to Discovery, terminate the Agreement to the extent it relates to the Services, which require use of the proposed Subcontractor.

11.3 If the Subcontractor is engaged without objection from Subscriber, Discovery will enter into a written agreement with each Subcontractor that complies with Data Protection Laws and imposes data protection obligations that are no less protective of Personal Data than Discovery's obligations under this DPA. Discovery will remain responsible for its Subcontractors' compliance with the obligations of this DPA and for any acts or omissions of such Subcontractor as if they were Discovery's acts or omissions. Discovery, upon request, will use reasonable efforts to provide Subscriber with copies of its Subcontractor agreements, provided that it may redact confidential information or other information it is legally or contractually prohibited from disclosing to Subscriber.

12. **Data Sharing Requirements**. Discovery acknowledges and agrees that FERPA limits the transfer and re-transfer of Educational Records and FERPA PII. Other than disclosing such information to a Subcontractor pursuant to Section 11, Discovery will not release, re-disclose or otherwise reveal, directly or indirectly, FERPA PII or Educational Records to any individual, agency, entity, or third party unless specifically authorized by Subscriber in writing.

13. **Assistance**. Discovery will provide reasonable assistance to Subscriber with (i) complying with Subscriber's obligations in relation to the security of Processing Personal Data and notification of a Personal Data Breach, (ii) any data protection assessments, and (iii) any investigations by competent data privacy authorities, in each case solely in relation to Processing of Personal Data by and taking into account the nature of the Processing and information available to Discovery. Discovery will provide to Subscriber all information reasonably necessary to demonstrate compliance with Data Protection Laws.

14. **Production of Records**. By not later than seven (7) days from the date of a written request by Subscriber, Discovery will provide to Subscriber all Educational Records pertaining to any student(s) identified in such request.

15. **Audits**. Subscriber shall have the right to take reasonable and appropriate steps to ensure that Discovery uses Personal Data in a manner consistent with Subscriber's obligations under Data Protection Laws, and to stop and remediate any such unauthorized use. In connection with this, Subscriber may request once per calendar year to audit Discovery's Security Policy and related systems that are used to store Personal Data in order to verify compliance with this DPA and the Data Protection Laws. If Subscriber wishes to conduct an audit using a third-party auditor, Discovery may object to Subscriber's choice of third-party auditor on reasonable grounds and in such event, Subscriber will select a different auditor. Subscriber will reimburse Discovery for any time expended in relation to such audit at Discovery's then-current hourly professional services rate. Subscriber and Discovery will mutually agree upon the scope and timing of an audit prior to any such audit. An audit performed pursuant to this Section 15 will not exceed one (1) business day and will not unreasonably interfere with the normal conduct of Discovery's business. Subscriber (or Subscriber's third-party auditor) will at all times comply with the use, security, and access policies at such location. Any audit performed pursuant to this Section 15 will be conducted under a confidentiality agreement and any information or report derived from such audit will be deemed Discovery's confidential information. Subscriber is responsible and fully liable for the actions and omissions of its personnel and authorized representatives while on Discovery's premises and/or inspecting Discovery's systems and facilities.

16. **Suspension**. Subscriber may suspend the transfer of Personal Data to Discovery, or terminate the affected Agreement without penalty to Subscriber if: (i) Discovery is in material breach of its obligations under this DPA and does not cure such breach within thirty (30) days of Subscriber's notification to Discovery of such breach; or (ii) Discovery notifies Subscriber that it cannot comply with the obligations set forth in this DPA or the Data Protection Laws.

17. **Term**. The term of this DPA will end simultaneously and automatically at the later of (i) the termination of the Agreement; or (ii) when all Personal Data is deleted from Discovery's systems.

18. **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 a Data Protection Law; or (ii) breach of any provision of this DPA.

19. **General**.

19.1 **Schedules**. All Schedules to this DPA are hereby incorporated by reference into, and made a part of, this DPA.

19.2 **Order of Precedence**. In the event of a conflict between the terms of this DPA, any Order Form, and the Agreement with respect to the subject matter herein, the following order of precedence shall apply: (i) this DPA; (ii) the Agreement; (iii) any Order Form.

19.3 **Survival**. The obligations set forth herein will survive termination of the Agreement and DPA for as long as Discovery Processes or stores Personal Data.

19.4 **Severability**. Should any provision of this DPA be deemed invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.

20. **Definitions and Interpretation**.

20.1. **Definitions**.

"**Business Purpose**" means the Services described in the Agreement and any Order Form, or any other purpose specifically identified in Schedule 6.

"**Data Protection Laws**" means:

(a) the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR part 99) ("**FERPA**");

(b) the Children's Online Privacy and Protection Act (15 U.S.C. §§ 6501–6506) ("**COPPA**");

(c) the Colorado Student Data Transparency and Security Act (C.R.S. 22-16-101 et.al.);

(d) the Connecticut Public Act 16-189;

(e) the California Consumer Privacy Act of 2018 ("**CCPA**");

(f) the California Student Online Student Information Protection Act (**SB-1177**) ("**SOPIPA**");

(g) the California Assembly Bill No. 1584;

(h) the New York State Education Law § 2-d;

(i) the Illinois Student Online Personal Protection Act ("**SOPPA**");

(j) the Canada Personal Data Protection and Electronic Documents Act ("**PIPEDA**"); and

(k) all other federal and state data protection and breach notification laws applicable to Personal Data being Processed by Discovery; in each case, as in force and applicable, and as may be amended, supplemented, or replaced from time to time.

"**Destroy**" means: (i) shredding; (ii) permanently erasing and deleting; (iii) degaussing; or (iv) otherwise modifying Personal Data in paper, electronic, or other means so as to make it unreadable, unreconstructible, and indecipherable.

"Educational Records" means "Education records," as defined under 34 C.F.R. § 99.3.

"**FERPA PII**" means "Personally Identifiable Information," as defined under 34 C.F.R. § 99.3. FERPA PII does not include de-identified data derived from Educational Records.

"**Law**" or "**Laws**" means all applicable federal, country, state, provincial, regional, territorial or local laws, and other laws, rules, and regulations (including, but not limited to, Data Protection Laws), ordinances, interpretive letters, and other official releases of or by any authority, decrees, orders, and codes (including any requirements for permits, certificates, approvals, and inspections), as the same are promulgated, supplemented, and/or amended from time to time.

"**Personal Data** " means: (i) information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, including, without limitation, any Student Data; or (ii) is otherwise personal information, personally identifiable information, personal data, covered information, or the applicable term as the term is defined under the applicable Data Protection Law(s).

"**Subcontractor**" means any person (including any entity or individual but excluding an employee of Discovery) appointed by or on behalf of Discovery to Process Personal Data under the Agreement.

"**Student Data**" means any Personal Data of a student that through the course of Subscriber's use of the Services is: (i) provided by a student, or the student's parent or legal guardian, to Discovery in the course of the student's, parent's, or legal guardian's use of Discovery's website, service, or application that is designed and marketed for K–12 school purposes; (ii) created or provided by an employee or agent of the K–12 school, school district, local education agency, or county office of education, to Discovery; or (iii) gathered by Discovery through the operation of Discovery's website, service, or application that is designed and marketed for K–12 school purposes and is descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"**Personal Data Request**" means a request made by Subscriber, a parent or legal guardian, or student to exercise any rights granted by the Data Protection Laws.

The terms "**Business**", "**Controller**", "**Process**", "**Processor**", "**Sale**", "**Share**", and "**Service Provider**" shall have the same meaning assigned to them under Data Protection Laws. The term "Controller" is deemed to include "Business," and the term "Processor" is deemed to include "Service Provider."

Schedule 1

DISCOVERY EDUCATION DATA SECURITY POLICY

This Security Policy ("Policy") describes, in general, (i) what steps Discovery takes to protect Personal Data that is provided to Discovery; (ii) how Personal Data may be used; (iii) with whom Discovery may share Personal Data, and (iv) the steps Discovery takes to protect the Personal Data. All capitalized terms not defined herein shall have the meaning set forth in the DPA.

No Personal Data is required for the use of any of the basic Discovery Education services, however, in the event Users elect to use any of the functionality within the Discovery Education services which provide personalized pages, individual accounts, other user-specific customization, or otherwise submit or upload information (all such data is generally limited to the following: school name, first name, last name, grade level, and Discovery generated username/password), all such Personal Data provided to Discovery will be protected in accordance with this Policy.

No school employee Personal Data is required for Professional Development Services other than first name and last name for the purposes of attendance logs.

I. DEFINITIONS

Capitalized terms referenced herein but not otherwise defined shall have the meanings as set forth below:

"Authorized Disclosee" means the following: (1) third parties to whom the Subscriber has given Discovery written approval to disclose Personal Data; (2) third parties to whom disclosure is required by law; and (3) if applicable, third party vendors working on Discovery's behalf or performing duties in connection with Discovery's services (e.g. hosting companies) and who are required to implement administrative, physical, and technical infrastructure and procedural safeguards in accordance with accepted industry standards.

"Authorized User" means a Discovery employee authorized by the Subscriber to access Personal Data in order to perform the Services under the Agreement.

II. PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION

Basic Privacy Protections

1. Compliance with Law and Policy. All Personal Data is handled, processed, stored, transmitted and protected by Discovery in accordance with all applicable federal data privacy and security laws (including FERPA) and with this Policy.

2. Training. Employees (including temporary and contract employees) of Discovery are educated and trained on the proper uses and disclosures of Personal Data and the importance of information privacy and security.

3. Personnel Guidelines. All Discovery employees are required to be aware of and work to protect the confidentiality, privacy, and security of Personal Data. Discovery, and its respective personnel do not access Personal Data except to comply with a legal obligation under federal or state law, regulation, subpoena, or if there is legitimate need for the information to maintain data systems or to perform required services under the Agreement. The following provides a general description of the internal policies to which Discovery and its respective personnel adhere:

   a. Limit internal access to Personal Data to Discovery personnel with proper authorization and allow use and/or disclosure internally, when necessary, solely to personnel with a legitimate need for the Personal Data to carry out the Services provided under the Agreement.
   b. Disclose Personal Data only to Authorized Disclosees.
   c. Access Personal Data only by Authorized Users.

d. When Personal Data is no longer needed, delete access to Personal Data.

e. Permit employees to store or download information onto a local or encrypted portable devices or storage only when necessary, and to create a written record for retention verifying that the information is encrypted and stored in password-protected files, and that devices containing the information have appropriate security settings in place (such as encryption, firewall protection, anti-virus software and malware protection).

f. Any downloaded materials consisting of Personal Data remain in the United States.

g. Prohibit the unencrypted transmission of information, or any other source of Personal Data, wirelessly or across a public network to any third party.

h. Upon expiration or termination of the Agreement, Discovery will Destroy all Personal Data previously received from Subscriber no later than sixty (60) days following such termination, unless a reasonable written request is submitted by Subscriber to Discovery to hold such information Personal Data. Each electronic file containing Personal Data provided by Subscriber to Discovery will be securely Destroyed. This provision shall apply to Personal Data that is in the possession of Discovery, Discovery employees/personnel and/or Authorized Disclosees.

Information Security Risk Assessment

Discovery periodically conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic, paper, or other records containing Personal Data maintained by Discovery; Discovery reports such risks as promptly as possible to Subscribers; and Discovery implements security measures sufficient to reduce identified risks and vulnerabilities. Such measures are implemented by Discovery based on the level of risks, capabilities, and operating requirements. These measures include, as appropriate and reasonable, the following safeguards:

1. Administrative Safeguards

a. Sanctions: Appropriate sanctions against Subcontractor personnel who fail to comply with Discovery's security policies and procedures.

b. System Monitoring: Procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.

c. Security Oversight: Assignment of one or more appropriate management level employees of Discovery to be responsible for developing, implementing, and monitoring of safeguards and security issues.

d. Appropriate Access: Procedures to determine that the access of Discovery personnel to Personal Data is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Discovery personnel who have access to Personal Data.

e. Employee Supervision: Procedures for regularly monitoring and supervising Discovery personnel who have access to Personal Data.

f. Access Termination: Procedures for terminating access to Personal Data when employment ends, or when an individual no longer has a legitimate need for access.

2. Physical Safeguards

a. Access to Personal Data: Procedures that grant access to Personal Data by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.

b. Awareness Training: On-going security awareness through training or other means that provide Discovery personnel (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training also addresses procedures for monitoring log-in attempts and reporting discrepancies, as well as procedures for safeguarding passwords.

c. Incident Response Plan: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.

d. Physical Access: Procedures to limit physical access to Personal Data and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed, including physical barriers that require electronic control validation (e.g., card access systems) or validation by human security personnel.

e. Physical Identification Validation: Access is physically safeguarded to prevent tampering and theft, including procedures to address control and validation of a person's access to facilities based on his or her need for access to Personal Data.

f. Operational Environment: Procedures that specify the proper functions to be performed, the manner in which they are to be performed, and the physical attributes of the surroundings of facilities where Personal Data is stored.
g. Media Movement: Procedures that govern the receipt and removal of hardware and electronic media that contain Personal Data into and out of a facility.

3. Technical Safeguards
   a. Data Transmissions: Technical safeguards, including encryption, to ensure Personal Data transmitted over an electronic communications network is not accessed by unauthorized persons or groups.
   b. Data Integrity: Procedures that protect Personal Data maintained by Discovery from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.
   c. Logging off Inactive Users: Inactive electronic sessions are designed to terminate automatically after a specified period of time.

Security Controls Implementation

Discovery has procedures addressing the acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the need for management and staff to understand their responsibilities and have the knowledge, skills and motivation necessary to fulfill their duties.

Security Monitoring

In combination with periodic security risk assessments, 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. Discovery also assesses on an ongoing basis whether controls are effective and perform as intended, including intrusion monitoring and data loss prevention.

Security Process Improvement

Based on Discovery's security risk assessments and ongoing security monitoring, Discovery gathers and analyzes information regarding new threats and vulnerabilities, actual data attacks, and new opportunities for managing security risks and incidents. Discovery uses this information to update and improve its risk assessment strategy and control processes.

Audit

Discovery acknowledges Subscriber's right to audit any Personal Data collected by Discovery and/or the security processes listed herein upon reasonable prior written notice to Discovery's principal place of business, during normal business hours, and no more than once per year. Discovery shall maintain records and documentation directly and specifically related to the Services performed under the Agreement for a period of three (3) years, unless otherwise stated in Section II(3)(h) of this Policy.

Breach Remediation

Discovery keeps Personal Data provided to Discovery secure and uses reasonable administrative, technical, and physical safeguards to do so. Discovery maintains and updates incident response plans that establish procedures in the event a breach occurs. Discovery also identifies individuals responsible for implementing incident response plans should a breach occur.

If Subscriber or Discovery determines that a breach has occurred, when there is a reasonable risk of identity theft or other harm, or where otherwise required by law, Discovery provides any legally required notification to affected parties as promptly as possible, and fully cooperates as needed to ensure compliance with all breach of confidentiality laws.

Discovery reports as promptly as possible to Subscriber (or its designees) and persons responsible for managing their respective organization's incident response plan any incident or threatened incident involving unauthorized access to or acquisition of Personal Data of which they become aware. Such incidents include any breach or hacking of Discovery's Electronic Data System or any loss or theft of data, other electronic storage, or paper. As used herein, "Electronic Data System" means all information processing and communications hardware and software employed in Discovery's business, whether or not owned by Discovery or operated by its employees or agents in performing work for Discovery.

Personnel Security Policy Overview

Discovery mitigates risks by:

1. Performing appropriate background checks and screening of new personnel, in particular those who have access to Personal Data.
2. Obtaining agreements from internal users covering confidentiality, nondisclosure and authorized use of Personal Data.
3. Providing training to support awareness and policy compliance for new hires and annually for personnel.

Schedule 2

DISCOVERY EDUCATION SUBCONTRACTOR LIST

Discovery Education has disclosed and currently discloses covered information (as defined in 105 ILCS 85/5) to certain Subcontractors to support the delivery of Services. The following is a list of Discovery Education's subcontractors:

Subcontractor Name
Ably Realtime Ltd.
Amazon Web Services, Inc.
Atlassian, Inc. (and its affiliates)
Buildscale, Inc. dba Vidyard
Carry Technologies, Inc. dba Hightouch
Clever, Inc.
FPT Software (and its affiliates)
Gainsight, Inc.
Google LLC.
Hound Technology, Inc. dba Honeycomb.io
Iterable, Inc.
Looker (Google LLC)
MessageBird UK Limited (formerly Pusher Ltd)
Microsoft Corporation
MongoDB, Inc.
Sage Intacct, Inc.
Salesforce.com, Inc.
Snowflake, Inc.
Widgix, LLC dba Alchemer
Zendesk, Inc.
Zoom Video Communications, Inc.

Schedule 3

MYSTERY SCIENCE SUBCONTRACTOR LIST

Mystery Science has disclosed and currently discloses covered information (as defined in 105 ILCS 85/5) to certain Subcontractors to support the delivery of its Services. The following is a list of Mystery Science's subcontractors:

Subcontractor Name
Atlassian, Inc. (and its affiliates)
Amazon Web Services, Inc.
Carry Technologies, Inc. dba Hightouch
FPT Software (and its affiliates)
Iterable, Inc.
Looker (Google LLC)
Microsoft Corporation
New Relic, Inc. (Heroku)
Sage Intacct, Inc.
Salesforce.com, Inc. (Heroku)
Twilio, Inc. (Sendgrid)
Wistia, Inc.

Schedule 4

DREAMBOX LEARNING SUBCONTRACTOR LIST

DreamBox Learning has disclosed and currently discloses covered information (as defined in 105 ILCS 85/5) to certain Subcontractors to support the delivery of its Services. The following is a list of DreamBox Learning's subcontractors:

Subcontractor Name
Action Verb LLC dba Files.com
Algorithmity LTD
Amazon Web Services, Inc.
Atlassian, Inc. (and its affiliates)
BairesDev LLC
Carry Technologies, Inc. dba Hightouch
Catalyte Inc.
ClassLink, Inc.
Clever, Inc.
Datadog, Inc.
Encora Digital LLC
FPT Software (and its affiliates)
Iterable, Inc.
Looker (Google LLC)
Microsoft Corporation
MongoDB, Inc.
Otus, LLC
Pendo.io, Inc.
Sage Intacct, Inc.
Snowflake, Inc.
Stripe, Inc.
Tableau Software, LLC
Zendesk, Inc.

Schedule 5

PIVOT SUBCONTRACTOR LIST

Pivot has disclosed and currently discloses covered information (as defined in 105 ILCS 85/5) to certain Subcontractors to support the delivery of its Services. The following is a list Pivot's subcontractors:

Subcontractor Name
AC PM LLC (Postmark)
Amazon Web Services, Inc.
Anthropic, PBC
Atlassian, Inc. (and its affiliates)
Avalara, Inc. (AvaTax)
Carry Technologies, Inc. dba Hightouch
ClassLink, Inc.
Clever, Inc.
FPT Software (and its affiliates)
Gainsight, Inc.
Google LLC
Intercom, Inc.
Looker (Google LLC)
Microsoft Corporation
MongoDB, Inc.
Sage Intacct, Inc.
Salesforce.com, Inc.
Snowflake, Inc.
Stripe, Inc.

Schedule 6

Description of Processing

Categories of individuals whose Personal Data is Processed: The categories of data subjects are as follows: Students, teachers and administrators ("Users").

Categories of Personal Data Processed: The categories of Personal Data are as follows: Student grade level, Name, e-mail, ID number, Username, Passwords, Student generated content, Teacher First/Last Name, Teacher e-mail, Teacher username/password, Teacher ID, Teacher Interest, Grade Taught, Class Name, Class ID, Class Description, School Year, Class Grade, Class Subject

The frequency of the Processing: Continuous for as long as Subscriber uses the Services.

Nature of the Processing: Discovery will collect, receive, store, retain, transmit, delete (as provided in this DPA, the Agreement, and/or Order Form(s)), and otherwise use Personal Data as needed to provide the Services.

Purpose(s) of the Processing: The purpose of the Processing is to facilitate Discovery's provision of the Services to Subscriber in accordance with the Agreement, this DPA, any Order Form(s), and applicable law.

The period for which Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: Discovery will Process Personal Data for as long as required to provide the Services.