DATA PROTECTION ADDENDUM

This Data Protection Addendum (**"Addendum"**) is attached to, forms a part of, and applies to all services provided by Contractor to District under, the Apex Learning Price Quote 14794 dated May 21, 2021 (the **"Contract"**) between School District No. 1 in the City and County of Denver and State of Colorado, d/b/a Denver Public Schools (**"District"**) and Apex Learning Inc. (**"Contractor"**) (the Addendum and the Contract are collectively referred to hereinafter as **"Agreement"**). This Addendum amends the Contract by adding to, deleting from and modifying the Contract as set forth herein. To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Contract and this Addendum, this Addendum shall govern and the terms of the Contract that conflict with this Addendum or are inconsistent with this Addendum shall be of no force or effect. In consideration of the mutual covenants, promises, understandings, releases and payments described in the Contract and this Addendum, the parties agree to amend the Contract by adding the following language:

1. Definitions

1.1. **"*Biometric Record*,"** as used in the definition of "Personally Identifiable Information," means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

1.2. **"*Designated Representative*"** means District or Contractor employees as specified on Schedule 1 to whom all notices required in this Addendum will be sent.

1.3. **"*District Data*"** means any Personally Identifiable Information, Record, Education Records, as defined herein, and all Personally Identifiable Information included therein or derived therefrom that is not intentionally made generally available by the District on public websites or publications but is made available directly or indirectly by the District to Contractor or that is otherwise collected or generated by Contractor in connection with the performance of the Services, as defined herein.

1.4. **"*De-identified Data*"** means District Data from which all Personally Identifiable Information, as defined herein, and attributes about such data, have been permanently removed so that no individual identification can be made.

1.5. **"*Education Records*"** means records, files, documents and other materials that: (a) contain information directly related to a student; and (b) are maintained by the District, or by a party acting for the District such as Contractor.

1.6. **"*End User*"** means individuals authorized by the District to access and use the Services as defined herein.

1.7. **"*Incident*"** means a suspected, attempted, or imminent threat of unauthorized access, use, disclosure, breach, modification, disruption or destruction to or of District Data.

1.8. **"*Mine District Data*"** means the act of searching through, analyzing, accessing, or extracting District Data, metadata, or information not necessary to accomplish the Services or purpose(s) of this Agreement for the benefit of the District.

1.9. **"*Personally Identifiable Information*"** or **"*PII*"** means information and metadata that, alone or in combination, is linked or linkable to a specific student so as to allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Personally Identifiable Information includes, but is not limited to: (a) the student's name; (b) the name of the student's parent or other family members; (c) the address or phone number of the student or student's family; (d) personal identifiers such as the student's state-assigned student identifier, social security number, student number or biometric record; (e) indirect identifiers such as the student's date of birth, place of birth or mother's maiden name; and (f) demographic attributes, such as race, socioeconomic information, and gender.

To the extent it is not already included in the definition hereinabove, PII also includes: (a) "personal information" as defined in the Colorado Open Records Act, C.R.S. 24-72-101 et seq. ("CORA"); (b) Personally Identifiable Information contained in student "education records" as that term is defined in the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; (c) "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) "nonpublic personal information" as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (e) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; and (f) other financial account numbers, access codes, and state- or federal-identification numbers such as driver's license, passport or visa numbers.

1.10. **"*Securely Destroy*"** means to remove District Data from Contractor's systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in National Institute of Standards and Technology ("NIST") SP 800-88 r1 (2014) or as amended Guidelines for Media Sanitization so that District Data is permanently irretrievable in Contractor's and its Subcontractors' normal course of business.

1.11. **"*Security Breach*"** means an event in which District Data is exposed to unauthorized disclosure, access, alteration or use or a system configuration that results in a documented unsecured disclosure, access, alteration or use, in a manner not permitted in this Addendum, which poses a significant risk of financial, reputational or other harm to the affected End User or the District.

1.12. **"*Services*"** means any goods or services acquired by the District from the Contractor under the Contract, including the provision of Contractor's web-based curriculum accessed by End Users through the Internet.

1.13. **"*Subcontractor*"** means Contractor's subcontractors or agents, identified on Schedule 2, as updated by Contractor from time to time in accordance with the requirements of

this Addendum, who Contractor has engaged to enable Contractor to perform its obligations under the Contract.

1.14. **"*Student Profile*"** means a collection of PII data elements relating to a student of the District.

2. Rights and License in and to District Data

District owns all rights, title, and interest in and to District Data and any and all now known or hereafter existing intellectual property rights associated therewith, and any derivative works thereof or modifications thereto, including without limitation, De-identified Data other than performance usage data. The District hereby grants to Contractor a limited, nonexclusive license to use District Data solely for the purpose of performing its obligations specified in the Contract. This Agreement does not give Contractor any rights, title, or interest implied or otherwise, to District Data or De-identified Data, except as expressly stated in the Contract.

3. Data Privacy

3.1 Use of District Data. Contractor shall use District Data only for the purpose of performing the Services and fulfilling its duties under the Contract.

3.2 Prohibited Uses of District Data. With the exception of De-identified Data that the District has agreed in writing to allow Contractor to use as specified in Section 3.5, Contractor shall not:

3.2.1 Use, sell, rent, transfer, distribute, alter, mine, or disclose District Data (including metadata) to any third party without the prior written consent of the District, except as required by law or as set forth in Colorado Act Section 22-16-109(2)(a);

3.2.2 Use District Data for its own commercial benefit, including but not limited to, advertising or marketing of any kind directed toward children, parents, guardians, or District employees, unless such use is specifically authorized by this Agreement or otherwise authorized in writing by the District;

3.2.3 Use District Data in a manner that is inconsistent with Contractor's privacy policy;

3.2.4 Use District Data to create a Student Profile other than as authorized or required by the Contract to perform the Services; or

3.2.5 Store District Data outside the continental United States unless Contractor has given the District Designated Representative advance written notice of where and how the servers are housed, managed, and secured, and that the security standards required herein can be achieved.

3.3 Qualified FERPA Exception. If Contractor will have access to Education Records containing District Data, the parties acknowledge that, for the purposes of this Agreement, pursuant to FERPA, Contractor constitutes a "school official" that the District has determined has "legitimate educational interests" in the District Education Records and PII disclosed pursuant to the Contract. Contractor and District agree to abide by their respective obligations under FERPA including the limitations and requirements imposed on school officials. Contractor warrants and represents that during the five-year period preceding the Effective Date of this Agreement, it has not been found in violation of FERPA by the U.S. Department of Education's Family Policy Compliance Office.

3.4 Subcontractor Use of District Data. Contractor may disclose District Data to Subcontractors engaged by Contractor, for use solely in a manner consistent with this Agreement, and solely pursuant to a written agreement that fulfils the requirements of Colorado Act Section 22-16-109(3)(b). Contractor shall ensure that its employees and Subcontractors who have potential access to District Data have undergone any background screening identified by District to Contractor in writing as a requirement for execution of this Agreement 3.5 Use of De-identified Data. Contractor may use De-identified Data for purposes of research, the improvement of Contractor's products and services, and/or the development of new products and services. In no event shall Contractor or Subcontractors re-identify or attempt to re-identify any De-identified Data or use De-identified Data in combination with other data elements or De-identified Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

3.6 Privacy Policy Changes. Prior to making a material change to Contractor's privacy policies, Contractor shall send District's Designated Representative written notice, which includes a clear explanation of the proposed changes.

3.7 Misuse/Unauthorized Release. Upon discovering the misuse or unauthorized release of Student Personally Identifiable Information held in connection with this Agreement by Contractor, a Subcontractor or a subsequent Subcontractor of Contractor, Contractor will notify the District as soon as possible, regardless of whether the misuse or unauthorized release is a result of a material breach of the terms of this Agreement.

4. Data Security

4.1 Security Safeguards. Contractor shall store and process District Data in accordance with commercial best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in SANS Top 20 Security Controls, as amended, to secure such data from unauthorized access, disclosure, alteration, and use. Contractor shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with all applicable federal and state data protection and privacy laws, regulations and directives, including without limitation C.R.S. § 22-16-101 *et seq.*, as well as the terms and conditions of this Addendum. Without limiting the foregoing, and unless expressly agreed to the contrary in writing, Contractor warrants that all electronic District Data will be encrypted in transmission and at rest in accordance with NIST Special Publication 800-57, as amended.

4.2 Risk Assessments. Contractor shall conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

4.3 Audit Trails. Contractor shall take reasonable measures, including audit trails, to protect District Data against deterioration or degradation of data quality and authenticity, and to ensure data is deidentified in accordance with this Addendum.

4.4 Verification of Safeguards. Upon District's written request, Contractor shall provide or make available to the District for review, one or more of the following, verifying Contractor's administrative, physical and technical safeguards are in compliance with industry standards and best practices: (1) a third-party network security audit report; (2) certification from Contractor indicating that an independent vulnerability or risk assessment of the Contractor's data security program has occurred; (3) district data has been deidentified by Contractor as set forth in the definition of Deidentified Data in section 1.3 of this Addendum.

4.5 Background Checks.

4.5.1 If Contractor does not provide direct services to students but has access to District Data, the Contractor and every person, including any subcontractor or agent of the Contractor, shall be required to have a criminal background check per Contractor's internal employment policies. "Direct services to students" includes, but is not limited to: instruction; physical, mental, and social health supports; transportation; and food services, which are provided to students at least one time per month during the school year.

4.5.2 If Contractor provides direct services to students and has access to student data, the Contractor and every person, including any subcontractor or agent of the Contractor, shall be required to have a criminal background check that meets the requirements of § 22-32-109.7, C.R.S. and other District requirements, including a fingerprint-based conviction investigation. Conducting a Colorado Bureau of Investigation criminal history check or a Name Check investigation for any person providing services under this Contract does not meet District requirements. The costs associated with the background checks are solely the Contractor's responsibility. Thereafter, any personnel, subcontractor, volunteer or agent hired or added during the term of this Contract shall satisfy the requirements set forth in this Section before performing services on Contractor's behalf. The Contractor shall make the background check results available upon request of the District in compliance with the provisions of § 24-72-305.3, C.R.S. The District also reserves the right to conduct its own criminal background check of every person before Services begin.

4.5.3 Notwithstanding the criminal background check requirement as set forth above, Contractor hereby certifies that no employee, subcontractor, volunteer or agent of the Contractor performing the Services has been convicted in Colorado or in any other State of a criminal offense involving: (i) the abuse, abduction, sexual molestation, physical or sexual assault on, or rape of a minor; or (ii) any crime involving exploitation of minors, including but not limited to, child pornography offenses or any crime of violence. Contractor shall notify the District immediately upon the discovery or receipt of any information that any person performing services on Contractor's behalf has been detained or arrested by a law enforcement agency of the

aforementioned crimes. Contractor understands that allowing any employee, subcontractor, volunteer or agent of the Contractor performing the Services who has been arrested or convicted of the aforementioned crimes to: (i) provide direct services to students, (ii) access student data, or (iii) enter onto District property, constitutes a material breach of this Contract and may result in the immediate termination of this Contract and referral to law enforcement for possible criminal charges, or additional civil sanctions pursuant to federal and state law. Misdemeanor conviction(s) may not necessarily result in the immediate termination of this Contract. Misdemeanor convictions are evaluated on a case-by-case basis, considering the nature and gravity of the offense, time elapsed since the offense, conviction, or time served, and the nature of the Services. Upon the District's request, Contractor shall provide documentation of every person performing the Services to substantiate the basis for this certification.

5. Security Incident and Security Breach

5.1 Security Incident Evaluation. In the event of an Incident, Contractor shall follow reasonable industry practices to investigate and resolve the Incident, and as appropriate take reasonable steps to prevent developments that may result in the Incident becoming a Security Breach, at Contractor's expense in accordance with applicable privacy laws.

5.2 Response. As soon as possible upon becoming aware of a Security Breach, Contractor shall notify the District Designated Representative in writing as set forth herein, take reasonable steps to investigate the Security Breach, and cooperate fully with the District's investigation of and response to the Security Breach, at Contractor's expense in accordance with applicable privacy laws. Except as otherwise required by law, Contractor shall not provide notice of the Security Breach directly to individuals whose Personally Identifiable Information was involved, to regulatory agencies, or to other entities, without first providing written notice to the District's Designated Representative. Notice under this Section 5.2 shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

5.3 Security Breach Report. If the District reasonably determines that Contractor has committed a Security Breach, then the District may request Contractor to submit, as soon as reasonably practicable but in any event in no less than 30 calendar days from discovery of such breach, a written report, and any supporting documentation, identifying (i) the nature of the Security Breach, (ii) the steps Contractor has executed to investigate the Security Breach, (iii) what District Data or PII was used or disclosed, (iv) who or what was the cause of the Security Breach, (v) what Contractor has done or shall do to remediate any deleterious effect of the Security Breach, and (vi) what corrective action Contractor has taken or shall take to prevent a future Incident or Security Breach. The District reserves the right to require Contractor to amend its remediation plans.

5.4 Effect of Security Breach. Upon the occurrence of a Security Breach, the District may terminate this Agreement in accordance with Section 8. The District may require Contractor to suspend all Services, pending the investigation and successful resolution of any Security Breach, and Contractor may be required to reimburse District all amounts paid for any period during which

Services were not rendered. Contractor acknowledges that, as a result of a Security Breach due to the failure of Contractor to comply with this Addendum or otherwise caused by Contractor, the District may also elect to disqualify Contractor and any of its Subcontractors from future contracts with the District.

5.3 Liability for Security Breach. In addition to any other remedies available to the District under law, contract or equity, Contractor shall reimburse the District in full for all direct damages (i.e., excluding indirect, incidental, consequential, special, or punitive damages) that were actually incurred by the District as a result of a any Security Breach due to the failure of Contractor (or Contractor's Subcontractors) to comply with this Addendum or otherwise caused by Contractor (or Contractor's Subcontractors). If required by law or contract, Contractor shall provide notification to individuals whose Personally Identifiable Information was compromised and regulatory agencies or other entities, in accordance with the applicable law or contract. Where a Security Breach is due to the failure of Contractor (or Contractor's Subcontractors) to comply with this Addendum or otherwise caused by Contractor (or Contractor's Subcontractors), Contractor shall provide one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during any Security Breach could be used to commit financial identity theft.

6. Response to Legal Orders, Demands or Requests for Data

6.1 Received by Contractor. Except as otherwise expressly prohibited by law, Contractor will comply with Colorado Act Section 22-16-109(3)(II) if Contractor receives any subpoenas, warrants, other legal orders, or legal demands or requests seeking District Data and, to the extent permitted by law, will immediately notify the District of same.

6.2 Received by District. If the District receives a subpoena, warrant, or other legal order, demand or request seeking District Data maintained by Contractor, including but not limited to a request pursuant to the Colorado Open Records Act, C.R.S. § 24-72-100.1 *et seq*., the District will promptly notify Contractor, and Contractor, at District's expense, will reasonably cooperate with District to facilitate the District's response, as permitted by and in accordance with applicable law.

6.3 Parent Request. If a parent, legal guardian or student contacts the District with a request to review or correct District Data, pursuant to FERPA or the Colorado Act, the District will promptly notify Contractor's Designated Representative and Contractor shall facilitate District's access to and correction of any factually inaccurate Student Personally Identifiable Information maintained by Contractor in response to such request, as , within ten calendar (10) days after receipt of District's notice. Conversely, if a parent, legal guardian or student contacts the Contractor with a request to review or correct District Data or PII, Contractor shall promptly notify the District.

6.4 Access to District Data. District shall have access to District Data through the Services.

7. Compliance with Applicable Law

7.1. Children's Online Privacy and Protection Act. If Contractor collects personal information (as defined in the Children's Online Privacy and Protection Act of 1998, 5 U.S.C. 6501 to 6505, and its implementing regulations ("COPPA")) from children under thirteen (13) years of age in performing the Services, Contractor warrants, represents, and covenants that such collection is and shall be for the use and benefit of the District and for no other commercial purpose. Contractor has provided District with written notice of its collection, use, and disclosure practices.

7.2 Compliance with Laws. Contractor and District each warrant that it will abide by all applicable laws, ordinances, rules, regulations, and orders of all governmental agencies or authorities having jurisdiction in connection with this Agreement, including but not limited to: COPPA; FERPA; Payment Card Industry Data Security Standards; Protection of Pupil Rights Amendment, 20 U.S.C. 1232h, 34 C.F.R. Part 98; Americans with Disabilities Act, and Federal Export Administration Regulations.

7.3 Americans with Disabilities Act. To the extent the District is required to provide accommodations in compliance with the Americans with Disability Act ("ADA"), Contractor will require that its system and services will, at a minimum, conform with all applicable laws, regulations and guidance that apply to accessibility in accordance with the ADA, Section 504 of the Rehabilitation Act of 1973, and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA guidelines; provided, however, Contractor will have no obligations with respect to such compliance as it relates to any portion of the system and services provided or developed by the District including District content.

8. Term and Termination

8.1 Term. This Addendum takes effect immediately as of the Effective Date, and remains in full force and effect until the successful completion of the services, unless earlier terminated under Sections 8.2, 8.3 or 12.3.

8.2 Subject to Sections 8.3 and 12.3, this Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Contract between the Parties. Alternatively, upon re-execution of the Contract by the authorized persons of District and Contractor, this Addendum shall also be revived and be of full force and effect.

8.3 Termination.

8.3.1 If Contractor commits a material breach of this Addendum that involves the misuse or unauthorized release of Personally Identifiable Information, the District shall determine whether to terminate this Agreement in accordance with District policy adopted and implemented pursuant to the Colorado Act. In addition, either party may terminate the Agreement (in the case of District, in accordance with District policies) if, at any time, the other party has materially breached any of the requirements of this Agreement and failed to cure such breach within thirty (30) days following written notice by the other party.

9. Data Transfer Upon Termination or Expiration

9.1 Destruction or Return of District Data. With the exception of De-identified Data that District has specifically agreed in writing to allow Contractor to use after termination or expiration of this Agreement, or District Data for which Contractor has specifically obtained consent from the parent, legal guardian or student to keep, no later than (30) calendar days after termination or expiration of this Agreement, Contractor shall certify in writing that all District Data and PII that Contractor collected, generated or inferred pursuant to the Contract ("Contract Data"), is securely returned or Securely Destroyed, pursuant to Schedule 4 attached hereto.

9.3 Response to Specific Data Destruction or Return Requests. After receiving a written request from the District, Contractor shall Securely Destroy or return any specific District Data or Contract Data that is in its possession or in the possession of its Subcontractors within five (5) business days, excluding national holidays, after receiving a written request from the District, provided that Contractor will not liable for any inability to perform the Services that arise due to any such request made during the Term.

10. Limitation of Liability and Indemnification

10.1 If either party is a "public entity" then it will be responsible for the negligent acts and omissions of its officers, agents, employees and representatives with respect to its obligations under this Agreement. Any provision of this Agreement, whether or not incorporated herein by reference, shall be controlled, limited and otherwise modified so as to limit any liability of the Contractor under the Colorado Governmental Immunity Act, C.R.S. 24-10-101 et seq. It is specifically understood and agreed that nothing contained in this paragraph or elsewhere in this Agreement shall be construed as an express or implied waiver of its governmental immunity or as an express or implied acceptance of liabilities arising as a result of actions which lie in tort or could lie in tort in excess of the liabilities allowable under the Act, as a pledge of the full faith and credit of the Partner, or as the assumption by the Partner of a debt, contract or liability of the District or its affiliates in violation of Article Xl, Section 1 of the Constitution of the State of Colorado.

10.2 Limitation of Liability. SUBJECT TO SECTION 10.1, CONTRACTOR WILL NOT BE LIABLE TO DISTRICT FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, EVEN IF CONTRACTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF SUCH POSSIBILITY WAS REASONABLY FORESEEABLE.

10.3 If Contractor is not a "public entity" then Contractor shall indemnify, defend and hold District and its elected officials, employees, representatives, and agents (**"Indemnified Parties"**) harmless, from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses, including reasonable attorneys' fees, the costs of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against any Indemnified Party to the extent arising out of or resulting from Contractor's, or Contractor's subcontractors, failure to comply with any of its obligations under this Addendum. These indemnification duties shall survive termination or expiration of this Addendum.

11. Insurance

11.1 Coverage. As required by Schedule 6.

12. Miscellaneous

12.1 No End User Agreements. In the event that the Contractor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with End Users, the parties agree that, as between the District and Contractor, in the event of a conflict between the terms of any such agreement and this Addendum, the terms of this Addendum and the Contract, in that order of precedence, shall control.

12.2 Public Inspection of Agreement. Contractor acknowledges and agrees that this Addendum and all documents Contractor provides District as required herein, are public records for purposes of the Colorado Open Records Act, C.R.S. § 24-72-100.1 *et seq.* and shall at all times be subject to public inspection. The parties understand that in the event of a request for disclosure of such information, the District will notify Contractor to give Contractor the opportunity to redact its proprietary or confidential material. In the event of the filing of a lawsuit to compel disclosure, the District will tender Contractor's material to the court for judicial determination of the issue of disclosure and Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure or waive the same.

12.3 Survival. The Contractor's obligations under Sections 3, 4, 5, 6, 9, and 10, and any other obligations or restrictions that expressly or by their nature are to continue after termination, shall survive termination of this Addendum for any reason until all District Data has been returned or Securely Destroyed.

12.4 Choice of Law. Any claim, controversy or dispute arising under or related to this Addendum shall be construed pursuant to the substantive, not conflicts, laws of the State of Colorado. Each of the Parties submits to the exclusive jurisdiction of any state court sitting in or federal court with jurisdiction over Denver County, Colorado, in any action or proceeding arising out of or relating to this Agreement and agrees that all claims in respect of the action or proceeding may be heard and determined in any such court. Each Party also agrees not to bring any action or proceeding arising out of or relating to this Addendum in any other court. Each of the Parties waives any defense of inconvenient forum to the maintenance of any action or proceeding so brought and waives any bond, surety or other security that might be required of any other Party with respect to any such action or proceeding.

12.5 Immunities. The District retains all of its rights, privileges and immunities under the Colorado Governmental Immunity Act, C.R.S. § 24-10-101 *et seq.*

12.6 No Assignment. Contractor shall not assign or subcontract any of its rights or obligations hereunder without the express written consent of District. Any assignment in violation of this section shall be void.

12.7 No Third Party Beneficiaries. Nothing in this Agreement shall be construed to give any rights or benefits to anyone other than District and Contractor.

12.8 Schedules. The following schedules are attached hereto, or shall be attached hereto, and are specifically made a part hereof by this reference:

Schedule 1 – Designated Representatives
Schedule 2 – Subcontractors
Schedule 3 – Written Consent to Maintain De-identified Data
Schedule 4 – Certification of Destruction\Return of District Data
Schedule 5 – Data Elements
Schedule 6 – Insurance

12.9 Counterparts. This Addendum may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

12.10 Effective Date. This Addendum will become effective when all parties have signed it. The date of this Addendum will be the date this Addendum is signed by the last party to sign it (as indicated by the date associated with the party's signature).

12.11 Electronic Signatures and Electronic Records. Each party consents to the use of electronic signatures by the other party. This Addendum, and any other documents requiring a signature under this Addendum, may be signed electronically by each party in the manner specified by the District. The parties agree not to deny the legal effect or enforceability of this Addendum solely because it is in electronic form or because an electronic record was used in its formation. The parties agree not to object to the admissibility of the Addendum in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party is signing this agreement on the date stated opposite that party's signature.

SCHOOL DISTRICT NO. 1 IN THE CITY AND COUNTY OF DENVER AND STATE OF COLORADO, D/B/A DENVER PUBLIC SCHOOLS

Date: 08/27/2021 By: _____

Staci Crum, Director, Financial Operations
DeeDee Case, Manager of Strategic Sourcing

Apex Learning Inc.

Date: 8/26/2021 By: _____

Chuck Lanphier
Sr. Vice President, Client Services

APPROVED AS TO FORM:
By: _____
Office of the General Counsel

OPTION 1

SCHEDULE 1
Designated Representatives

NOTICE REQUIRED	DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Security Breach:	**Robert Losinski** **Manager, Info Security** **By U.S. Mail: 780 Grant St** **Denver, CO 80203** **By E-mail: infosec@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
FERPA Records Requests:	**Jennifer Collins** **Chief Privacy Officer, Deputy General Counsel** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: legal_contracts@dpsk12.org** **Records Requests: https://denverco.scriborder.com/**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
CORA Requests:	**Stacy Wheeler** **CORA Officer** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: cora@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
Updates to Privacy Policy / Transparency Requirements:	**Jennifer Collins** **Chief Privacy Officer, Deputy General Counsel** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: legal_contracts@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
Updates to Subcontractor Schedule:	**Jennifer Collins** **Chief Privacy Officer, Deputy General Counsel** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: legal_contracts@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
Data Retrieval:	**Robert Losinski** **Manager, Info Security** **By U.S. Mail: 780 Grant St** **Denver, CO 80203** **By E-mail: infosec@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
Destruction of Data:	**Robert Losinski** **Manager, Info Security** **By U.S. Mail: 780 Grant St** **Denver, CO 80203** **By E-mail: infosec@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**

OPTION 2

SCHEDULE 1
Designated Representatives

DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Name: **Jennifer Collins** **Title:** **Chief Privacy Officer, Deputy General Counsel** **Address:** **1860 Lincoln St** **Denver, CO 80203** **Phone:** **720-423-2211** **E-mail:** **legal_contracts@dpsk12.org**	**Name:** **Chuck Lanphier** **Title:** **Senior Vice President, Client Services** **Address:** **1215 Fourth Avenue, Suite 1500** **Seattle, WA 98161** **Phone:** **206-381-5600** **E-mail:** **salesdocs@apexlearning.com**

SCHEDULE 2
Subcontractors

Contractor shall update this information as necessary to maintain accuracy and shall send revised attachments, exhibits or schedules to the District's Authorized Representative.

What third party vendors does Contractor do business with that may have access to student personally identifiable data, and what is the purpose of these third party vendors (please fill complete the table below with this information)?

Name of Subcontractor	**Primary Contact Person**	**Subcontractor's Address**	**Subcontractor's Phone/email**	**Purpose of re-disclosure to Subcontractor**
Amazon Web Services				Cloud-based storage and hosting
Microsoft Corporation				Cloud-based storage, business productivity applications
Salesforce.com				CRM
SolarWinds Worldwide, LLC				Application performance monitoring
Threat Stack, Inc.				Infrastructure security and monitoring
Veracode				Application security

SCHEDULE 3
Written Consent to Maintain De-identified Data

The District hereby gives its consent for Contractor to retain and use for the stated purpose and period, De-identified Data elements as set forth below:

Description of De-identified Data Elements	**Purpose for Retention and Use**	**Period of Use**

I\We, _____, as [title] _____ and the authorized representative(s) of the Contractor do hereby certify that no attempt will be made to re-identify De-identified Data.

Contractor Name: _____

Contractor Representative Name: _____

Title: _____

Signature: _____ Date: _____

SCHEDULE 4
Certification of Destruction\Return of District Data

I\We, _____[NAME(S)]_____, as the authorized representative(s) of the Contractor do hereby acknowledge and certify under penalty of perjury that [initial next to both subparts of the applicable Part A or Part B]:

Part A - Destruction:

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was destroyed on _____, 20___ by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was destroyed as set forth below:

Name of Subcontractor	*Date of Deletion*	*Destruction Method*

Part B - Return: [If this option is elected by the District, then Contractor shall also complete Part A.]

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District, on _____, 20___ to _____, by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District as set forth below:

Name of Subcontractor	*Date of Return*	*Return / Transfer Method*

Contractor Name: _____

Contractor Representative Name: _____

Title: _____

Signature: _____ Date: _____

SCHEDULE 5
Data Elements

(Mandatory to be completed if Service Provider is a School Service Contract Provider under CRS 22-16-101 et seq.)

1. **Service Provider collects, generates or uses pursuant to the Agreement the following data elements of District Data or PII**:

Application Technology Meta Data: IP Addresses of users, Use of cookies, etc.
Application Use Statistics: Meta data on user interaction with application.
Communications: Online communications captured (emails, blog entries).
Parent/Guardian Contact Information: Email.
Student Contact Information: Email.
Student Identifiers: Local (School district) ID number, Provider/App assigned student ID number; Student app username; Student app passwords.
Student Name: First and/or Last.
Student App Performance: Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level).
Student work: Student generated content; writing, pictures, etc.
Transcript: Student course grades, Student course data, Student course grades/ performance scores.

2. **Service Provider collects and uses the District Data for the following educational purposes**:

Access to Apex Learning digital curriculum and professional development in support of our digital curriculum.

3. **Service Provider's policies regarding retention and disposal of District Data are as follows**:

Upon termination of services, all personal identifiable information for pupil records is removed.

4. **Service Provider uses, shares or discloses the District Data in the following manner:**

5. **Has Service Provider's agreement has ever been terminated by another school district for failure to comply with the same or substantially similar security obligations as those set forth in this Agreement**?

   ☐ Yes ☑ No.

   If yes, describe: