EXHIBIT A, CONFIDENTIALITY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION AGREEMENT
Purchase Order: 2018-0637

This Confidentiality Agreement ("Agreement") is part of the attached Purchase Order between the State of Colorado, Colorado Department of Education and the Contractor. For purposes of this Agreement, the State is referred to as "CDE", "State", and "Department" and the Contractor is referred to as "Contractor."

RECITALS

A. Department wishes to disclose certain information to Contractor pursuant to the work being performed by Contractor, some of which may constitute Student Personally Identifiable Information ("PII") or Educator Data (defined below).

B. Department and Contractor intend to protect the privacy and provide for the security of Student Personally Identifiable Information and Educator Data disclosed to Contractor pursuant to this Purchase Order. Contractor shall adhere to 22-16-101 *et. al.*, C.R.S.; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g; and 34 C.F.R. Part 99.

C. The Department is required to enter into a contract, this Agreement, containing specific requirements with Contractor prior to the disclosure of Student Personally Identifiable Information or Educator Data, as set forth in, but not limited to, 22-16-101 *et. al.*, C.R.S.; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g; and 34 C.F.R. Part 99, and the requirements contained in this Agreement.

The parties agree as follows:

A. Definitions

1. "Aggregate Data" means data collected and reported at the group, cohort, or institutional level that is aggregated using protocols that are effective for preserving the anonymity of each individual included in the data.

2. "Data" includes Student Personally Identifiable Information and Educator Data.

3. "Destroy" means to remove Data from Contractor's systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in NIST Special Publication 800-88 Guidelines for Media Sanitization so that the Data is permanently irretrievable in the Contractor's and Subcontractor's normal course of business.

4. "Educator Data" includes, but is not limited to, the educator's name; any unique identifier, including social security number; and other information that, alone or in combination, is linked or linkable to a specific educator.

5. “Incident” means an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources of the State pursuant to C.R.S. Section 24-37.5-401 et seq. Incidents include, but are not limited to (i) successful attempts to gain unauthorized access to a State system or Student Personally Identifiable Information, Educator Data, or State Confidential Information regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a State system for the processing or storage of data; or (iv) changes to State system hardware, firmware, or software characteristics without the State’s knowledge, instruction, or consent.

6. “State Confidential Information” means all information, data, records, and documentary materials, regardless of physical form or characteristics, which are of a sensitive nature and belong to the State, including but not limited to any non-public State records, sensitive State data, protected State data, State personnel records and other information or data concerning individuals, which has been communicated, furnished, or disclosed by the State to Contractor. Notwithstanding the foregoing, State Confidential Information shall not include Student Personally Identifiable Information or Educator Data and shall not include information required to be disclosed pursuant to the Colorado Open Records Act, CRS §24-72-101, et seq.

7. "Student Personally Identifiable Information (PII)" means information that is collected, maintained, generated, or inferred and that, alone or in combination, personally identifies an individual student or the student's parent or family. Student Personally Identifiable Information includes, but is not limited to a student's name; the name of a student's parent or other family member; the address of a student or student's family; a personal identifier such as a student's social security number, student number, or biometric record; other indirect identifiers such as a student's date of birth, place of birth, and mother's maiden name; a student’s email address, cell phone number or any other information that allows physical or online contact with a student; a student’s discipline or criminal records; a student’s juvenile dependency records; a student’s medical or health records including, without limitation, records regarding a student’s disabilities; a student’s socioeconomic information, political affiliations, or religion; a student’s text messages, IP address, or online search activity; a student’s photos and voice recordings; a student’s food purchases; or geolocation information.

   Student Personally Identifiable Information also includes data that is collected and stored by CDE at the individual student level and is included in a student’s educational record and includes State-administered assessment results, including participation information, courses taken and completed, credits earned and other transcript information; course grades and grade point average; grade level and expected graduation year; degree, diploma credential attainment or other school exit information; attendance and mobility information between and within Colorado school districts; special education data and special education discipline reports limited to object information that is sufficient to produce the federal Title IV annual incident report; date of birth, full name, gender, race, and ethnicity; and program participation information required by state or federal law.

8. "Subcontractor" means any third party engaged by Contractor to aid in performance of Contractor's obligations.

9. "Targeted Advertising" means selecting and sending advertisements to an individual based on information obtained or inferred over time from the individual's online behavior, use of applications, or Data. Targeted Advertising does not include advertising to an individual at an online location based on the individual's current visit to that location or in response to the individual's request for information or feedback and is without the collection and retention of an individual's online activities over time. Targeted Advertising also does not include adaptive learning, personalized learning, or customized education.

B. General Provisions

1. The State reserves all right, title, and interest to State system data, State Confidential Information, Data, and all related data and content.

2. Contractor shall comply with all laws and regulations concerning confidentiality of State Confidential Information and Data including, but not limited to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g; 34 C.F.R. Part 99 and the Student Data Transparency and Security Act, C.R.S. Section 22-16-101 et. seq. Contractor shall immediately forward to the State's principal representative any request or demand from a third party for State Confidential Information or Data in the possession of Contractor.
3. Upon request of the State or of the Colorado State Board of Education, Contractor shall submit its data processing facilities for an audit of the measures referred to in this Agreement by the State or by a State approved delegate.
4. Contractor shall send the State a written notice which includes a clear explanation of the proposed changes prior to making a material change to Contractor's privacy policies.

C. Confidentiality of State Confidential Information

1. Contractor shall notify its agents, employees, Subcontractors, and assigns who may come into contact with State Confidential Information that each is subject to the confidentiality requirements set forth in this Purchase Order, before permitting them to access State Confidential Information.

2. State Confidential Information shall not be distributed or sold to any third party or used by Contractor or its agents except as authorized by this Purchase Order or as approved in writing by the State. Contractor shall provide and maintain a secure environment that ensures confidentiality of all State Confidential Information wherever located. State Confidential Information shall not be retained by Contractor or its agents except as permitted in this Purchase Order or approved in writing by the State.

3. Disclosure of State Confidential Information by Contractor for any reason may be cause for legal action by third parties against Contractor, the State or their respective agents. Contractor shall indemnify, save, and hold harmless the State, its employees and agents, against any and all costs, expenses, claims, damages, liabilities, and court awards (including attorney fees and costs), incurred by the State in relation to any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees in connection with State Confidential Information.

D. Subcontractors

1. Contractor shall not use a Subcontractor or disclose Data to a Subcontractor unless and until the Contractor contractually requires the Subcontractor to comply with C.R.S. §§22-16-108 through 22-16-111 and the requirements of this Agreement.
2. If Contractor discovers that Subcontractor or any subsequent subcontractor has committed a material breach of the contract between Contractor and Subcontractor that involves the misuse or unauthorized release of Data, Contractor acknowledges that the State may terminate the Purchase Order with Contractor unless Contractor terminates the contract with Subcontractor as soon as possible after Contractor knows or has reason to know of Subcontractors' or any subsequent subcontractors' material breach.
3. Upon discovering the misuse or unauthorized release of Data held by a Subcontractor or any subsequent Subcontractor, Contractor shall notify CDE and the Office of Information Security ("OIS") within forty-eight (48) hours, regardless of whether the misuse or unauthorized release by the Subcontractor is a result of a material breach of the terms of the Purchase Order or results in an Incident.
4. No later than thirty (30) days after the execution of the Purchase Order, Contractor shall provide the State with information detailing the purpose and the scope of the contract between the Contractor and all Subcontractor(s) and the types and uses of Data that Subcontractor(s) holds under the contract between the Contractor and Subcontractor(s) other than technical Vendors in the ordinary course of business who perform services under Contractor's supervision on Contractor's own system.

5. Contractor shall not maintain or forward Data to or from any other facility or location except for backup and disaster recovery purposes. Any backup or disaster recovery contractor that can access Data shall be considered a Subcontractor that must comply with the Subcontractor requirements in this Agreement.

E. End of Agreement

1. Should Contractor not comply with the requirements of this Section and that non-compliance results in the misuse or unauthorized release of Data by the Contractor, the State may terminate the Purchase Order immediately as provided under this Purchase Order and in accordance with C.R.S. Section 22-16-105(5).

2. Upon written request by the State made before or within thirty (30) calendar days after termination of the Purchase Order, Contractor shall make available to the State a complete and secure (i.e. encrypted and appropriately authenticated) download file of all data, including, but not limited to, all Data, State Confidential Information, schema and transformation definitions, or delimited text files with documented, detailed schema definitions along with attachments in its native format.

3. Following the termination of this Purchase Order and upon Contractors receipt of written request, Contractor shall, within thirty (30) calendar days, Destroy all Data and State Confidential Information collected, generated, or inferred as a result of this Purchase Order. The Contractor shall notify the State of the date upon which all of the Data and State Confidential Information is Destroyed.

4. The State retains the right to use the established operational services to access and retrieve Data and State Confidential Information stored on Contractor's infrastructure at its sole discretion.

F. Use

1. The Contractor shall not use or share Data beyond the purposes set forth as follows:

   a. To carry out the Contractor's responsibilities listed in the Purchase Order Statement of Work.

2. In the event the Purchase Order requires Contractor to store, process or transfer Data, Contractor shall store, process, and transfer Data only in or to facilities located within the United States.

3. During the term of this Purchase Order, if the State requests the destruction of Data collected, generated or inferred as a result of this Purchase Order, the Contractor shall Destroy the information within five (5) calendar days after the date of the request, except for backups. Contractor can retain a student's PII provided that:

   a. The Contractor obtains the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian to retain the student's PII; or

   b. The student has transferred to another state and the receiving state has requested that the Contractor retain the student's PII.

4. If Contractor seeks to share or publically release Data without complying with the requirements of this Agreement for Subcontractors or without complying with the de-identification processes outlined in Contractor's Data Handling Policy (Exhibit C), Contractor shall provide a summary of the intended use to CDE and CDE shall agree to this use in writing.

G. Incident

1. If Contractor becomes aware of an Incident, misuse of Data, or unauthorized disclosure involving any Data, it shall notify the CDE and OIS within one (1) calendar day and cooperate with the State regarding recovery, remediation, and the necessity to involve law enforcement, if any.

2. Unless Contractor can establish that Contractor or any of its Subcontractors is not the cause or source of the Incident, Contractor shall be responsible for the cost of notifying each person whose personal information may have been compromised by the Incident.

3. Contractor shall determine the cause of an Incident and produce a remediation plan to reduce the risk of incurring a similar type of breach in the future. Contractor shall present its analysis and remediation plan to the State within ten (10) calendar days of notifying the State of an Incident. The State reserves the right to adjust this plan, in its sole discretion. If Contractor cannot produce its analysis and plan within the allotted time, the State, in its sole discretion, may perform such analysis and produce a remediation plan, and Contractor shall reimburse the State for the reasonable costs thereof.

4. Disclosure of Data by Contractor or any Subcontractor for any reason may be cause for legal action by third parties against Contractor, the State, or their respective agents. Contractor shall indemnify, save, and hold harmless the State, its employees, and agents against any and all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred as a result of any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees pursuant to this Agreement. Notwithstanding any other provision of this Purchase Order, Contractor shall be liable to the State for all direct, consequential and incidental damages arising from an Incident caused by Contractor or its Subcontractors.

5. In the event of an Incident, Contractor shall provide the State or its designated representatives with access seven (7) days a week, twenty-four (24) hours a day, for the purpose of evaluating, mitigating, or resolving the Incident.

H. Disallowed Activities

A Contractor that uses, creates or acquires Data shall not knowingly engage in any of the following activities:

1. Contractor shall not collect, use or share Data for any purpose not specifically authorized by the Purchase Order. Contractor may use Data for a purpose not strictly authorized by the Purchase Order only with the written consent of the State and, for uses of PII not authorized by the Purchase Order, with the written consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian.

2. Contractor shall not use Data in a manner or disclose Data to any third party that is materially inconsistent with the Contractor's privacy policy, except as stated in subsection 3, below, of this Article X, Section H.

3. Contractor may use Data in a manner that is inconsistent with Contractor's privacy policy without violating the terms of this Purchase Order provided that the use does not involve selling or using Data for Targeted Advertising or creating a personal profile of the student or educator, and the use is for one or more of the following purposes:

    a. To ensure legal or regulatory compliance or to take precautions against liability.

    b. To respond or to participate in the judicial process.

    c. To protect the safety of users or others on Contractor's website, online service, online application, or mobile application.

    d. To investigate a matter related to public safety.

    If Contractor uses or discloses Data in accordance with this Section H.3., Contractor shall notify the State within two calendar days of the use or disclosure of the Data.

4. Contractor shall not sell Data, except that this prohibition does not apply to the purchase, merger, or other type of acquisition of the Contractor, or any assets of the Contractor, by another entity, so long as the successor entity continues to be subject to the provisions of this Purchase Order.

5. Contractor shall not use or share Data with any party for the purposes of Targeted Advertising to students or educators.

6. Contractor shall not use Data to create a personal profile of a student or educator other than for supporting the purposes authorized by the State or, for uses of PII, with the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian.

I. Data Security

1. Contractor shall maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality and integrity of Data. At a minimum, the information security program shall include the requirements listed in this Section I– Data Security. In addition to these requirements, Contractor shall review, on a semi-annual basis, all OIS policies and procedures which OIS has promulgated pursuant to C.R.S. Sections 24-37.5-401 through 406 and 8 C.C.R. Section 1501-5 and posted at http://oit.state.co.us/ois, to ensure compliance with the standards and guidelines published therein. Contractor must comply with all obligations within all OIS policies for the high risk categorization. All Data received from CDE shall be considered part of the High data security category and Contractor shall comply with all requirements in OIS policies and procedures required for data categorized as High. Contractor shall cooperate, and shall cause its Subcontractors to cooperate, with the performance of security audit and penetration tests by OIS or its designee. In the event of conflicts or inconsistencies between this Agreement Confidential Information and OIS policies and procedures, such conflicts or inconsistencies shall be resolved by giving priority to this Agreement. Confidential Information.

2. Contractor shall provide physical and logical protection for all related hardware, software, applications, and data that meet or exceed industry standards and requirements as set forth in this Purchase Order. Contractor shall take full responsibility for the security of all Data in its possession, and shall hold the State harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof. Contractor shall provide for the security of such Data, in a form acceptable to the State, including, without limitation, non-disclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, network firewalls, intrusion detection (host and network), data security logging and monitoring systems, and audits.

3. Contractor shall provide the State or its designated representatives with access, subject to Contractor's reasonable access security requirements, for the purpose of inspecting and monitoring access and use of Data, maintaining State systems, and evaluating physical and logical security control effectiveness.

4. Contractor shall perform, in a form reasonably acceptable to the State, current background checks on all of its respective employees and agents performing services or having access to Data provided under this Purchase Order. The background checks must include, but are not limited to the following areas: County, State, National and Federal Criminal Records and a Sex Offender Registry Search. A background check shall be conducted at the time of hire and Contractor shall require all Contractor employees to notify Contractor of any criminal convictions that occur after the date of hire. Contractor shall remove an employee's access to CDE Data if he or she is convicted of any crime.

5. Contractor shall have strong access controls in place.

6. Workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended.

7. Contractor shall protect all Data with a complex password. Contractor shall ensure passwords are confidential and prohibit the sharing of passwords. Passwords must not be written down or stored in an unsecure location. Contractor shall periodically change passwords and shall ensure passwords are not reused. Contractor shall have password locks for laptops and mobile devices.

8. Contractor shall disable and/or immediately delete unused and terminated user accounts. Contractor shall periodically assess account inactivity for potential stale accounts.

9. Contractor shall not share Data on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes, unless they are sharing this data with a school, with only individuals who are authorized to view that Data, and contains Data only from that school or that District as a whole.

10. Contractor shall implement annual intrusion penetration/vulnerability testing.

11. Contractor shall encrypt Data at rest on central computing systems. Contractor shall also encrypt any backup, backup media, removable media, tape or other copies. In addition, Contractor shall fully encrypt disks and storage for all laptops and mobile devices.

(a) Contractor may maintain backups of State data and destroy them in accordance with its Data Handling Practices.

12. Contractor shall provide annual, mandatory security awareness and Data handling training for all of its employees/independent contractors handling Data pursuant to this Purchase Order.

13. Contractor shall install and maintain on computers accessing or processing Data appropriate endpoint security anti-virus and anti-malware software. Contractor shall ensure all Contractor's data processing systems, servers, laptops, PCs, and mobile devices are regularly scanned and have all security patches applied in a timely manner.

14. Contractor shall use a secure method such as Secure File Transfer Protocol (SFTP) or comparable method to transmit Data. Contractor shall never send Data via email or transport Data on removable media.

15. Contractor shall have physical security in buildings housing Data, along with controlled physical access to buildings and/or data centers.

16. Contractor's devices used to copy or scan hard copies of Data must have encrypted storage. Contractor shall scrub storage devices when equipment is retired. Hard copies containing Data are discouraged and must be physically secured, not left unattended, and physically Destroyed.

17. Contractor shall protect Data stored in cloud based systems in the same manner as local Data. Use of free cloud based services is prohibited. Contractor shall use secondary encryption to protect Data in cloud storage. Cloud environments, when employed by Contractor, must be fully documented by Contractor and open to CDE inspection and verification remotely and under Contractor direction. Access to Contractor's cloud based computing environments is only permitted via restricted access, by VPN or least privileged access lists, and never accessible directly via the Internet.

J. Transparency Requirements

1. Contractor acknowledges that the State will post this Purchase Order to the State's website.

2. If Contractor collects, stores or accesses PII, Contractor must comply with the following requirements for transparency:

    a. No later than thirty (30) calendar days after the signing of this Purchase Order, Contractor shall provide the State with information detailing the purpose and the scope of the Purchase Order, the types of PII that Contractor holds under this Purchase Order, and the uses of PII under this Purchase Order. Contractor will send this information to dataprivacy@cde.state.co.us.

    b. Contractor shall facilitate access to and correction of any factually inaccurate student PII in response to a request from a local education provider or from the State.

c. Contractor shall provide transparency to parents, school districts and the public about its collection and use of PII including posting the following information on its public website:

   i. Contact information for an individual within Contractor's organization that can provide information on or answer questions related to the use of PII by Contractor.

   ii. An explanation of how PII will be shared with Subcontractors or disclosed to any third party.

   iii. The types of PII Contractor collects, generates, or uses. This information must include all PII that is collected regardless of whether it is initially collected or ultimately held individually or in the aggregate.

   iv. An explanation of the PII, an explanation of how the PII is used, and the learning purpose for which the PII is collected and used.

   Contractor shall update this information on its website as necessary to maintain accuracy. The Contractor acknowledges that the State will post this information on its public website.

K. INSURANCE

Contractor and its Subcontractors shall obtain and maintain insurance as specified in this section at all times during the term of this Contract. All policies evidencing the insurance coverage required hereunder shall be issued by insurance companies satisfactory to Contractor and the State. For the purposes of this agreement, vendors used by Contractor in the ordinary course of business that perform general software and content development services for Contractor, under Contractor's supervision, for the benefit of all its customers and not specifically for CDE shall not be considered Subcontractors.

<u>Contractors and Subcontractors</u>

Contractor shall obtain and maintain during the term of this Contract insurance coverage and policies meeting the same requirements set forth in the section below. In addition, Contractor shall require each contract with subcontractors other than those that are public entities, providing Goods or Services in connection with this Contract, to include insurance requirements substantially similar to the following:

<u>Worker's Compensation</u>

Worker's Compensation Insurance as required by State statute, and Employer's Liability Insurance covering all of Contractor or subcontractor employees acting within the course and scope of their employment.

<u>General Liability</u>

Commercial General Liability Insurance written on ISO occurrence form CG 00 01 10/93 or equivalent, covering premises operations, fire damage, independent contractors, products and completed operations, blanket contractual liability, personal injury, and advertising liability with minimum limits as follows: (a) $1,000,000 each occurrence; (b) $1,000,000 general aggregate; (c) $1,000,000 products and completed operations aggregate; and (d) $50,000 any one fire.

If any aggregate limit is reduced below $1,000,000 because of claims made or paid, subcontractor shall immediately obtain additional insurance to restore the full aggregate limit and furnish to Contractor a certificate or other document satisfactory to Contractor showing compliance with this provision.

Automobile Liability

Automobile Liability Insurance covering any auto (including owned, hired and non-owned autos) with a minimum limit of $1,000,000 each accident combined single limit.

Cyber Privacy Liability

Contractor agrees to maintain Cyber Privacy Insurance for claims and losses with respect to network, internet (cloud) or other data disclosure risks (such as data breaches, releases of confidential information, unauthorized access/use of information, and identity theft) with minimum limits of not less than $1,000,000 per occurrence and $2,000,000 aggregate.

Additional Insured

The State shall be named as additional insured on all Commercial General Liability and Automobile Liability Insurance policies (leases and construction contracts require additional insured coverage for completed operations on endorsements CG 2010 11/85, CG 2037, or equivalent) required of Contractor and any subcontractors hereunder.

Primacy of Coverage

Coverage required of Contractor and subcontractor shall be primary over any insurance or self-insurance program carried by Contractor or the State.

Cancellation

The above insurance policies shall include provisions preventing cancellation or non-renewal without at least thirty (30) days prior notice to Contractor and Contractor shall forward such notice to the State within seven (7) days of Contractor's receipt of such notice.

Subrogation Waiver

All insurance policies in any way related to this Contract and secured and maintained by Contractor or its subcontractors as required herein shall include clauses stating that each carrier shall waive all rights of recovery, under subrogation or otherwise, against Contractor or the State, its agencies, institutions, organizations, officers, agents, employees, and volunteers.

Certificates

Contractor and all subcontractors shall provide certificates showing insurance coverage required hereunder to the State within seven (7) days of the Effective Date of this Contract. No later than fifteen (15) days prior to the expiration date of any such coverage, Contractor and each subcontractors shall deliver to the State or Contractor certificates of insurance evidencing renewals thereof. In addition, upon request by the State at any other time during the term of this Contract or any sub-contract, Contractor and each subcontractors shall, within ten (10) days of such request, supply to the State evidence satisfactory to the State of compliance with the provisions of this Section XIII.

L. Exclusions:

This Agreement does not:

1. Impose a duty on a provider of an interactive computer service, as defined in 47 U.S.C Sec. 230, to review or enforce compliance with this Purchase Order.

2. Impede the ability of a student to download, export, or otherwise save or maintain his or her own PII or documents.

3. Limit internet service providers from providing internet connectivity to public schools or to students and their families.

4. Prohibit a Contractor from marketing educational products directly to parents so long as the marketing does not result from the use of PII obtained by the Contractor as a result of providing its services under this Purchase Order.

5. Impose a duty on a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this Purchase Order on that software or those applications.

M. This Agreement does not prohibit Contractor's use of PII to:

1. Use adaptive learning or design personalized or customized education.

2. Maintain, develop, support, improve, or troubleshoot a Contractor's website, online service, online application, or mobile application.

3. Provide recommendations for school, education, or employment purposes, provided Contractor does not receive any payment or other consideration from a third party to make or support the recommendation.

4. Respond to a student's request for information or feedback provided Contractor does not receive any payment or other consideration from a third party for the information or feedback.

5. Identify, for a student, institutions of higher education or scholarship providers that are seeking students who meet specific criteria, only if Contractor has obtained the written consent of the student or the student's parent or legal guardian. Contractor may use PII for this purpose regardless of whether the institutions of higher education or scholarship providers provide payment or other consideration to the Contractor.

6. In accordance with the terms of this Purchase Order, produce and distribute, free or for payment or other consideration, student class photos and yearbooks only to the State, students, parents, or individuals authorized by parents.

7. Provide for the student, only with the express written consent of the student or the student's parent or legal guardian given in response to clear and conspicuous notice, access to employment opportunities, educational scholarships or financial aid, or postsecondary education opportunities, regardless of whether the Contractor receives payment or other consideration from one or more third parties in exchange for the PII. This exception applies only to Contractors that provide nationally recognized assessments that postsecondary institutions of higher education use in making admissions decisions.

N. Authorized Representative

1. CDE designates Contractor as an Authorized Representative under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g; and 34 C.F.R. Part 99.

2. CDE will disclose to Contractor

3. Student first and last name, date of birth, gender, student school enrollment, student grade level, teacher name, and other personally identifiable data CDE discloses Data to Contractor for the purposes of carrying out an audit or evaluation of Federal- or State-supported education programs or to enforce or to comply with Federal legal requirements that relate to those programs. Data will be used for the purposes stated in the Purchase Order between CDE and Contractor and will be governed by the terms of this Addendum.

4. Contractor shall only disclose Data to Subcontractors who are designated as Authorized Representatives and who have legitimate interests in the audit or evaluation of a Federal- or State-supported education program or for compliance or enforcement of Federal legal requirements related to these programs.

Signature

Persons signing for Contractor hereby swear and affirm that they are authorized to act on Contractor's behalf and acknowledge that the State is relying on their representations to that effect.

Contractor Legal Name:	Curriculum Associates, LLC
Signature of Authorized Officer or Agent:	
Typed or Printed Name of Authorized Officer or Agent:	David Caron
Title of Authorized Officer or Agent:	Chief Financial Officer
Date:	3/7/2018