CEC STUDENT DATA PRIVACY ADDENDUM

This Data Privacy Addendum ("DPA") is entered into by and between **Colorado Early Colleges** (hereinafter referred to as "LEA"), and **[Name].** (hereinafter referred to as "Provider") on August 1, 2020. The parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide LEA and/or schools controlled by or falling under the administrative jurisdiction of LEA with certain digital educational services ("Services") as described in Article I and Exhibit "A"; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide or cause to be provided certain documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") 20 U.S.C. § 1232g; Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501-6502; Protection of Pupil Rights Amendment ("PPRA"), 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. § 1400 *et seq.*; and

WHEREAS, the documents and data transferred from LEA and created by the Provider's Services are also subject to certain State of Colorado laws and regulations pertaining to student data privacy, including the Student Data Transparency and Security Act ("SDTSA"), C.R.S §§ 22-16-*101 et. al.*; and

WHEREAS, the parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit "C") transmitted to Provider from the LEA pursuant to Exhibit "A", including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, and SDTSA. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

2. **Nature of Services Provided**. The Provider has agreed to provide the digital educational services described in Exhibit "A".

3. **Student Data to Be Provided**. In order to perform the Services described in this Article and Exhibit "A", LEA shall provide the categories of data described in the Schedule of Data, attached hereto as Exhibit "B".

4. **DPA Definitions**. The definitions of terms used in this DPA are found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or any other Pupil Records transmitted to the Provider pursuant to this DPA is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data or Pupil Records. The parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this DPA shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. The Provider will cooperate and provide Student Data within ten (10) days at the LEA's request. Provider may transfer Pupil-Generated Content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall cooperate and respond within five (5) days to the LEA's request for Personally Identifiable Information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.

4. **Third Party Request**. Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to

any Third Party or allow any Third Party to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not include De-Identifiable Information or anonymous usage data regarding a student's use of the Services.

5. No Unauthorized Use. Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.

5.1 Provider shall not collect, use or share Student Data for any purpose not specifically authorized by the DPA. Provider may use Student Data for a purpose not strictly authorized by the DPA only with the written consent of the LEA and with the written consent of the student (provided the student is over 18) or the student's parents or legal guardian.

5.2 Provider shall not use Student Data in a manner or disclose Student Data to any third party that is materially inconsistent with the Provider's privacy policy.

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

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

5.3.2 To respond or to participate in the judicial process.

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

5.3.4 To investigate a matter related to public safety.

5.4 If Contractor uses or discloses PII in accordance with Section G.3., Contractor shall notify the LEP within two calendar days of the use or disclosure of the PII.

5.5 Contractor shall not sell PII, 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 Contract.

5.6 Contractor shall not use or share PII with any party for the purposes of Targeted Advertising to students.

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

6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data in manner consistent with C.R.S. §§22-16-108 through 22-16-110 and the terms of this DPA.

   6.1 If Provider discovers that Subprocessors or any subsequent subprocessor has committed a material breach of the DPA between Provider and Subprocessor that involves the misuse or unauthorized release of PII, Provider acknowledges that the LEA may terminate the DPA with Provider unless Provider terminates the DPA with Subprocessor as soon as possible after Provider knows or has reason to know of Subprocessors' or any subsequent subprocessors' material breach.

   6.2 Upon discovering the misuse or unauthorized release of PII held by a Subprocessor or any subsequent Subprocessor, Provider shall notify LEA within one calendar day, regardless of whether the misuse or unauthorized release by the Subprocessor is a result of a material breach of the terms of the DPA or results in an Incident.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws**. LEA shall provide data for the purposes of the DPA in compliance with FERPA, COPPA, PPRA, IDEA, and SDTSA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."

2. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

3. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all State of Colorado and federal laws and regulations pertaining to the privacy and security of Student Data and the handling of any breach or unauthorized release of PII, including FERPA, COPPA, PPRA, IDEA, and SDTSA.

2. **Authorized Use**. Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than to carry out the Providers responsibilities as stated in this DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, any meta data, user content or other non-public information and/or PII contained in the Student Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.

4. **No Disclosure**. De-Identifiable Information, as defined in Exhibit "C", may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify De-Identifiable Information and not to transfer De-Identifiable Information to any party unless (a) that party agrees in writing not to attempt re-identification, or (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA.

5. **Disposition of Data**. Provider shall dispose, delete, or de-identify, in accordance with NIST Special Publication 800-88, all Personally Identifiable Information obtained under the DPA when it is no longer needed for the purpose for which it was obtained. During the term of this DPA, if the LEA requests the destruction of a Student's Data collected, generated or inferred as a result of this DPA, the Provider shall destroy the information within five (5) calendar days after the date of the request unless: the Provider 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 Data; or the student has transferred to another public education entity and the receiving public education entity has requested that the Provider retain the Student Data. Upon request by LEA made before or within thirty (30) calendar days after termination of this DPA, Provider shall make available to the LEA a complete and secure download file of all data, including, but not limited to, all Student Data and PII, schema and transformation definitions, or delimited text files with documented, detailed schema definitions along with attachments in its native format. Following the termination of this DPA, Provider shall, within thirty (30) calendar days, destroy all PII and collected, generated, or inferred as a result of this DPA. Nothing in the DPA authorizes Provider to maintain PII beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the data has been disposed. The duty to dispose of Student Data shall not extend to De-Identifiable Information or data placed in a separate Student account, pursuant to the other terms of the DPA.

6. **Advertising Prohibition**. Provider is prohibited from using Student Data to (a) inform, influence, or enable Targeted Advertising to students or families/guardians; (b) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Services; or (c) develop commercial products or services unrelated to the Services provided to Client.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to maintain and abide by a comprehensive information security program that includes appropriate administrative, technological, and physical safeguards consistent with industry best practices to protect the security, privacy,

confidentiality, and integrity of Student Data. General security duties of Provider are as follows:

a. Passwords and Employee Access. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

b. Security Protocols. Each party agrees to maintain security protocols that meet industry best practices regarding the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.

c. Employee Training. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

d. Security Technology. When the Services are accessed using a supported web browser, Secure Socket Layer or equivalent technology shall be employed to protect data from unauthorized access. The Services security measures shall include server authentication and data encryption. All data shall be encrypted in transmission and at rest in accordance with NIST Special Publication 800-57, as amended. Provider shall host all Services data in SOC 2 compliant environments located within the United States of America.

e. Subprocessors Bound. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V and in accordance with applicable federal and state regulations. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

f. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

g. Backups. Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

h. Audits. Upon receipt of a reasonable request from the LEA, the Provider will allow the LEA to audit, at LEA's expense, the security and privacy measures that are in place to

ensure protection of the Student Record or any portion thereof. The Provider will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide full access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within one (1) calendar day of the incident and cooperate with the LEA regarding recovery, remediation, and the necessity to involve law enforcement, if any. 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. Incidents include, but are not limited to (i) successful attempts to gain unauthorized access to a LEA system or Student Data regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a LEA system for the processing or storage of data; (iv) a material breach of the DPA that involves the misuse or unauthorized release of Student Data; or (v) changes to LEA system hardware, firmware, or software characteristics without LEA's knowledge, instruction, or consent. Provider shall follow the following process:

   2.1 The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice. Unless Provider can establish that Provider or any of its Subproviders is not the cause or source of the Incident, Provider shall be responsible for the notification cost.

   2.2 The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

      2.2.1 The name and contact information of the reporting LEA subject to this section.

      2.2.2 A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

      2.2.3 If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

      2.2.4 Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

2.2.5 A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

2.3 At LEA's discretion, the security breach notification may also include any of the following:

2.3.1 Information about what the agency has done to protect individuals whose information has been breached.

2.3.2 Advice on steps that the person whose information has been breached may take to protect himself or herself.

2.4 Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including PII and agrees to provide LEA, upon request, with a copy of said written incident response plan.

2.5 At the request and with the assistance of LEA, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated. Should Provider not comply with the requirements of this DPA and that non-compliance results in the misuse or unauthorized release of Student Data by the Provider, the LEA may terminate the DPA immediately as provided under this DPA and in accordance with CRS 22-16-107(2)(a).

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall dispose of all of LEA's data pursuant to Article IV, section 5.

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA, COPPA, PPRA, IDEA, and SDTSA. In the event there is conflict between the terms of the DPA and any other writing, such as Provider's service agreement, terms of service, or privacy policy, the terms of this DPA shall apply and take precedence. Except as described in this paragraph, all other provisions of any other agreement shall remain in effect.

5. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or

agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

6. Public Inspection of Agreement. Provider acknowledges and agrees that this DPA and all documents Provider provides LEA as required herein, are public records and may at all times be subject to public inspection.

6.1 Provider shall facilitate access to and correction of any factually inaccurate Student Data or PII in response to a request from a local education provider or from the LEA.

6.2 Provider acknowledges that the LEA will post this DPA to the LEA's website.

6.3 Provider shall provide transparency to parents, school districts, and the public about its collection and use of Student Data including posting the following information on its public website:

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

6.3.2 An explanation of how the PII will be shared with Subproviders or disclosed to any third party.

6.3.3 The types of PII that are collected, generated, or used by the Provider. This information must include all PII that is collected regardless of whether it is initially collected or ultimately held individually or in the aggregate.

6.3.4 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.

6.4 Provider shall update this information on its website as necessary to maintain accuracy.

7 **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8 **Successors Bound**. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation, or other business reorganization or sale of all or substantially all of the assets of such business.

9 **Governing Law; Venue and Jurisdiction**. This DPA will be governed by and construed in accordance with the laws of State of Colorado, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction to the state and federal courts located in El Paso County, Colorado for any dispute arising out of or relating to this DPA or the transactions contemplated hereby.

10 **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11 **Multiple Counterparts:** This DPA may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this DPA. In proving this DPA, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this DPA by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

IN WITNESS WHEREOF, the parties have executed this Data Privacy Addendum as of the last day noted below.

For and on behalf of:	For and on behalf of:
Colorado Early Colleges	**[Name of DSP]**
By: _____	By: _____
Name: _____	Name: _____
Title: Head of School	Title: _____
Date: _____	Date: _____

EXHIBIT "A"

DESCRIPTION OF SERVICES

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses, Use of cookies etc.	
	Other application technology meta data Specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data (specify): *Student Personality Assessments*	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information Specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information (specify):	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	

Category of Data	Elements	Check if used by your system
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information(specify): *First Generation College Student*	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID No.	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In-App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT "C"

DEFINITIONS

De-Identifiable Information: The term "De-Identifiable Information" refers to data and information for which all Personally Identifiable Information has been removed or obscured in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider's specific steps to de-identify the data will depend on the circumstances but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de-identified if there are fewer than twenty (20) students in the samples of a particular field or category, e.g., less than twenty students in a particular grade or less than twenty students of a particular ethnicity.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, Student Data, metadata, and user or Pupil-Generated Content obtained by reason of the use of the Services, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, indirect identifiers that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty, and the following:

- First Name
- Last Name
- Home Address
- Email Address
- Date of Birth
- Telephone Number
- Social Security Number
- Educational Records
- Special Education Data
- Grades
- Evaluations
- Test Results
- Biometric Information
- Geolocation Information
- Socioeconomic Information
- Political Affiliations
- Religious Information
- Discipline Records
- Juvenile Dependency Records
- Criminal Records
- Medical Records
- Health Records
- Text Messages
- Search Activity
- Photos
- Videos
- Voice Recordings
- Documents Student Identifies

Pupil Generated Content: The term "Pupil-Generated Content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: The term "Pupil Records" means (1) any information that directly relates to a pupil that is maintained by LEA; and (2) any information acquired directly from a pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee.

School Official: For the purposes of this DPA and pursuant to 34 CFR 99.31(B), the term "School Official" means is a contractor that: (1) performs an institutional service or function for which the agency or institution would otherwise use employees; (2) is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) is subject to 34 CFR 99.33(a) governing the use and re-disclosure of PII from student records.

Student Data: The term "Student Data" includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that, alone or in combination, personally identifies an individual student or the student's parent or family, and is descriptive of the 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 allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data includes Pupil Records for the purposes of this DPA and for the purposes of State of Colorado and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. De-Identifiable Information or anonymous usage data regarding a student's use of the Services shall not be considered Student Data. Student Data also includes other information that, alone or in combination, is linked or linkable to a specific student that would 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; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Subprocessor: The term "Subprocessor" means a Third Party that Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

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

Third Party: The term "Third Party" means an entity that is not the Provider or LEA.