DATA PROTECTION AGREEMENT (DPA)

DISTRICT:	**Jefferson County School District** 1829 Denver West Drive, Bldg. 27 Golden, Colorado 80401
DATA RECIPIENT:	
DATA RELEASE PURPOSE:	
EFFECTIVE DATE:	The date of the Data Recipient's signature.
DESIGNATED REPRESENTATIVE	**DESIGNATED REPRESENTATIVE:** Chief Information Officer And

The Data Recipient agrees to the terms of the DPA by signing below.
Individuals signing on behalf of the Data Recipient represent and warrant that they are authorized to bind the party for which they are signing.

<Data Recipient Name>
By: _____
Signature
Print Name: _____

Title: _____

The District has or intends to share, release, make accessible, or otherwise make District Data available to the Data Recipient for the Data Release Purpose under the conditions and Data Recipient's agreement set forth herein.

This DPA:

1. Governs the privacy, protection, integrity, and security of District Data that comes into Data Recipient's possession or is otherwise made accessible to the Data Recipient through the District's use of Digital Services.
2. Controls the Data Recipient's handling of District Data.
3. Provides for the Parties' response in case of a data breach or other incidence.
4. Ensures compliance with applicable state and federal laws and industry standards.

5. **Defined Terms**. Capitalized words that are used throughout the DPA and that are capitalized outside of English grammar rules have the meaning ascribed to them:
   5.1. In the DPA section titled *"Definitions"* and
   5.2. In the Purchasing Contract Definitions to be accessed on the District's Purchasing webpage and
   5.3. When first used and then defined in parentheses and quotation marks anywhere in the DPA and the Contract.

   In the event of a conflict or inconsistency between and among these definition sources, the DPA definitions prevail for purposes of interpretation of the DPA.

6. **Duration of the DPA**. The Data Recipient's duties under the DPA begin at the earlier of the Effective Date or when the Data Recipient receives District Data. The DPA remains in effect for as long as the District provides District Data to the Data Recipient or the Data Recipient possesses or otherwise controls District Data, whichever is longer.

7. **Designated Representative**. Each Party designates an individual, office holder, or title holder to act as the Designated Representative for Legal Notices required by this DPA. The Designated Representatives are those listed on the cover page of this DPA.

8. **Data Ownership**.
   8.1. District Data is District property and continues to be District property when disclosed to the Data Recipient.
   8.2. In connection with District Data, the District also owns:
      8.2.1. All now and hereafter existing intellectual property rights associated with District Data, and
      8.2.2. De-identified Data, and
      8.2.3. Any derivative works thereof or modifications thereto.

8.3. In addition, Students may claim and continue to claim ownership rights in their respective Student-Generated Content, and this DPA does not affect or modify the rights of Students in their Student-Generated Content.

9. **License Grant**. The District grants to the Data Recipient a limited, non-exclusive, revocable license to use District Data solely for performing its obligations under or otherwise fulfilling the Release Purpose and in accordance with the terms of this DPA and applicable law.

10. **Data Collection and Use**.
    10.1. Collection and Use. The Data Recipient shall collect only such District Data and other data and information that the Data Recipient needs to fulfill the Release Purpose and use it only to perform the services, deliver the goods, grant the licenses, or engage in such other activities as contemplated by the Data Release Purpose.
    10.2. No Re-Disclosure. The Data Recipient shall not disclose, transfer, release, share, or otherwise provide District Data to Persons except as expressly permitted by the DPA.
    10.3. Expressly Prohibited. In using the District Data, the Data Recipient shall **not**:
        10.3.1. Use, sell, rent, transfer, distribute, alter, Mine, or disclose District Data to any Person without the prior written consent of the District, except as (1) required by law or (2) permitted by the Colorado Student Data Law or (3) in connection with an entity merger or acquisition as permitted by C.R.S. §22-16-109(2)(a).
        10.3.2. Use District Data for its own commercial benefit outside of the consideration provided by the DPA.
        10.3.3. Engage in Targeted Advertising or any advertising, marketing, or surveying of any kind directed toward Students, parents, guardians, families or District employees and agents.
        10.3.4. Create a Student Profile.
        10.3.5. Use District Data in a manner that is inconsistent with its own Privacy Policy.

11. **Security**.
    11.1. Storage Location. When the District so requests, the Data Recipient shall provide to the District a complete and accurate list of the location of data centers and other places where the Data Recipient stores District Data upon the District's request.
    11.2. Security Safeguards. The Data Recipient shall store and process District Data in accordance with prevailing industry and commercial standards and practices. Storage shall secure data from unauthorized access, disclosure, alteration, and use. All safeguards, including without limitation the way District Data is collected, accessed, used, stored, processed, disposed of, and disclosed,

shall comply with all applicable federal and state data protection and privacy laws, regulations, and directives and the terms and conditions of this DPA.

11.3. Security Procedures. The Data Recipient shall implement and maintain reasonable security procedures and practices that are designed to help protect PII from Unauthorized Activity.

11.4. Encryption. The Data Recipient shall cause electronic District Data to always be encrypted in transmission and at rest in accordance with either (1) the latest NIST Special Publication, or (2) such other standard as the Parties may agree to in writing.

11.5. Risk Assessments. The Data Recipient shall conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

11.6. Audit Trails. The Data Recipient shall conduct audit trails and take such other reasonable measures to protect District Data against deterioration or degradation of data quality and authenticity.

11.7. Verification of Safeguards. When the District so requests, the Data Recipient shall verify that the Data Recipient's administrative, physical, and technical safeguards comply with industry standards by making the following available to the District for review:

11.7.1.1. A third-party network security audit report, or

11.7.1.2. Certification from the Data Recipient indicating that an independent vulnerability or risk assessment of the Data Recipient's data security program has occurred.

11.8. No Re-identification of De-identified Data. The Data Recipient shall not re-identify or attempt to re-identify and shall prohibit its Subcontractors from re-identifying or attempting to re-identify De-identified Data. The Data Recipient shall not use De-identified Data in combination with other data elements or De-identified Data in the possession of a Subcontractor so as to allow for re-identification.

11.9. Subcontractor Click-Through. If the Data Recipient is providing its Service using Subcontractors, and Click-Through will be required for the District to avail itself of the Services contemplated by the Contract, then the Data Recipient shall cause the Subcontractor providing such software or on-line access to consent to and honor the terms of this DPA with respect to District Data and the District's use of the services provided through the Subcontractor.

12. **Compliance with Data-Specific Laws**.

12.1. FERPA and Qualified FERPA Exception. If the Data Recipient will have access to Education Records, the Data Recipient is designated as a "school official" with "legitimate educational interests," (as these terms are defined by FERPA). The Data Recipient shall comply with the FERPA limitations and requirements imposed on school officials. The Data Recipient will use the Education Records only for the purpose of fulfilling its duties under the DPA and the Data Release Purpose for the District's and its End Users' benefit. The Data Recipient shall not share District

Data with or disclose it to any Person except as provided for in the Contract or the DPA, as required by law, or if authorized in writing by the District. The Data Recipient warrants and represents that during the five-year period preceding the Effective Date of the Contract, the Data Recipient has not been found in violation of FERPA by the Family Policy Compliance Office.

12.2. Colorado Student Data Law. the Data Recipient shall comply with its obligations under the Colorado Student Data Law if and to the extent the Data Recipient provides a "school service" or is a "school service contract provider," as these terms are used and defined by the Colorado Student Data Law, or to the extent the Data Recipient is otherwise subject to the Colorado Student Data Law. Obligations include, without limitation, those listed as follows, and in the event of a conflict between this list and the actual language of the Colorado Student Data Law, the latter prevails:

12.2.1. To provide clear information explaining the Student PII elements collected, the learning purpose for which Student PII is collected, and how the Data Recipient uses and shares the collected Student PII, all of which is as stated in ***Attachment 1*** **to the DPA (Data Elements)**, if completed, or as the Data Recipient has otherwise disclosed in separate writing to the District in connection with the District's data security review processes. C.R.S. §22-16-108(1).

12.2.2. To send to the District updates concerning the information about data element collection, use, and sharing so as to maintain accuracy. C.R.S. §22-16-108(1).

12.2.3. To provide clear notice to the District **before** making material changes to its Privacy Policy. C.R.S. §22-16-108(2).

12.2.4. Facilitate access to and correction of any factually inaccurate Student PII. C.R.S. §22-16-108(3).

12.2.5. Notify the District of misuse or unauthorized release of Student PII held by the Data Recipient or any Subcontractor as soon as possible after discovery. C.R.S. §22-16-108(4).

12.2.6. Obtain the consent of the Student or Student's authorized parent before using Student PII in a manner that is materially inconsistent with its Privacy Policy, the Contract, or the DPA. C.R.S. §22-16-109(1)(b).

12.2.7. Implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information disclosed to the Data Recipient and reasonably designed to help protect PII from unauthorized access, use, modification, disclosure, or destruction. C.R.S. §22-16-110(1).

12.3. Data Recipient's Privacy Policy. The Data Recipient shall comply with its Privacy Policy. Any changes to the Privacy Policy while the Agreement is in effect shall not result in less protection to the District than provided for in the Privacy Policy in effect on the Effective Date. To the extent the Colorado Student Data Law applies, the Data Recipient shall comply with its prior notice requirements regarding changes to the Privacy Policy.

12.4. Subcontractor and Employee Compliance. The Data Recipient is responsible for its employees' and Subcontractors' collection and use of and access to District Data and shall ensure their compliance with the terms of the DPA. The Data Recipient shall also ensure that its Subcontractors carry insurance coverage against cybersecurity and data breach risks as needed to cover their potential liability when performing under the DPA or to at least the same extent as the Data Recipient does and is required to under the DPA, whichever is greater. To the extent necessary to perform its obligations relating to the Data Release, the Data Recipient may disclose District Data to Subcontractors pursuant to a written agreement, specifying the purpose of the disclosure and holding Subcontractors accountable in such a manner that the District Data remains protected to the same or greater extent as if the Subcontractor and the Data Recipient were the same entity. If the Data Recipient is a school service contract provider, as defined by the Colorado Student Data Law, the Data Recipient shall disclose District Data to Subcontractors only in accordance with the requirements of the Colorado Student Data Law, including, without limitation, C.R.S. §22-16-109(3)(b).

12.5. Compliance with Laws. In addition to the laws cited elsewhere in the DPA, the Data Recipient shall comply with all laws that apply and to the extent they apply, and with all orders of governmental entities having jurisdiction over the Data including, most relevantly and without limitation, as appliable:

12.5.1. COPPA: The federal Children's Online Privacy Protection Act.
12.5.2. PPRA: the federal Protection of Pupil Rights Amendment.
12.5.3. The Colorado Website Accessibility law known as HB 21-1110 and regulations promulgated thereunder.
12.5.4. HIPAA: the federal Health Insurance Portability and Accountability Act.
12.5.5. The federal Health Information Technology for Economic and Clinical Health Act.
12.5.6. The federal Gramm-Leach-Bliley Financial Modernization Act of 1999.
12.5.7. The federal Americans with Disabilities Act.
12.5.8. Federal Export Administration Regulations.
12.5.9. The Colorado Privacy Act.

13. **Data Transfer: Return, Destruction, Migration**.

13.1. Specific Requests. At any time while the Data Recipient or their Subcontractors are in possession of District Data, the Data Recipient shall, upon the District's request and following the District' reasonable instructions take all, any one, or a combination of these actions:

13.1.1.1. Provide access to District Data;
13.1.1.2. Securely Destroy, return, or migrate District Data, using such methods and formats as the District requires;
13.1.1.3. Transfer, at the District's expense (unless the transfer is the result of default by the Data Recipient under the DPA or a Security Incident or Security Breach), District Data to any Person without significant interruption in service and in collaboration with

transferees to ensure that the transfer or migration facilities and methods are compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District continues to have reasonable access to District Data during the transition; or

13.1.1.4. Provide a mechanism for the District to transfer Student-Generated Content to a separate account created or otherwise controlled by each Student who generated the content.

13.2. The District to Direct Disposal. When the Data Release Purpose expires or otherwise terminates for any reason, the Data Recipient shall follow the District's direction concerning return or other disposal of District Data in the Data Recipient's or their Subcontractors' possession.

13.2.1. ***Return***. If the District directs the Data Recipient to return the District Data, then the Data Recipient shall transmit the District Data completely, accurately, in a secure manner, and in the format as the District directs and at a minimum in a format that allows the District to reasonably access the District Data. The Data Recipient shall then Securely Destroy all copies and back-ups of the District Data, except that the Data Recipient may retain copies and back-ups if and then only to the extent and for as long as required by law.

13.2.2. ***Destruction***. If the District directs the Data Recipient to destroy the District Data, the Data Recipient shall Securely Destroy all copies and back-ups of the District Data, except that the Data Recipient may retain copies and back-ups if and then only to the extent and for as long as required by law.

13.2.3. ***If No Direction***. If the District does not provide direction regarding the disposal of District Data, then the Data Recipient shall Securely Destroy the District within a reasonable amount after the end of the Contract or Data Release Purpose, whichever occurs later, except that the Data Recipient may retain copies and back-ups if and then only to the extent and for as long as required by law. The Data Recipient shall send written notice to the District at least 30 calendar days before the planned destruction date.

13.2.4. ***Subcontractors***. The Data Recipient shall cause its Subcontractors to Securely Destroy District Data within a reasonable amount of time after the end of the Contract or Data release purpose, except that Subcontractors may retain copies and back-ups if and then only to the extent and for as long as required by law.

13.2.5. ***Certificate of Destruction***. The Data Recipient shall provide to the District Designated Representative written certifications concerning the Securely Destroying of District Data, consistent with fact, and as and in such format as the District may request. If the Data Recipient is a School Service Contract Provider, then the Data Recipient shall notify the District in writing as of the date when all Student PII has been Securely Destroyed. C.R.S. §22-16-110 (3).

13.3. Survival. The provisions of this section titled *"Data Transfer: Return, Destruction, Migration"* survive the termination of the Contract and Data Release Purpose for as long as necessary to fully complete the obligations set forth herein.

14. **Security Incidents and Response**.

14.1. In the event of a Security Incident, the Data Recipient shall follow prevailing industry practices to fully investigate and resolve the Security Incident and take steps to prevent developments that may result in the Security Incident becoming a Security Breach, at the Data Recipient's expense and in accordance with applicable laws.

14.2. The Data Recipient shall notify the District Designated Representative in writing promptly after learning of a Security Breach, shall fully investigate the Security Breach, shall cooperate fully with the District's investigation of and response to the Security Breach, and use best efforts to prevent any further Security Breach at the Data Recipient's expense and in accordance with applicable laws. Except as may be otherwise required by law, the Data Recipient shall notify the District Designated Representative and obtain the District's approval in writing **before** the Data Recipient sends notice of the Security Breach directly to individuals whose PII was involved, to regulatory agencies, or to other entities.

14.3. If the District reasonably determines that the Data Recipient is fully or partly responsible for a Security Breach or is otherwise subject to or involved with a Security Breach, then the Data Recipient shall submit to the District, within 7 calendar days after the District so requests, a written report with supporting documentation that identifies, at a minimum:

14.3.1. The nature of the Security Breach.

14.3.2. The steps the Data Recipient has executed to investigate the Security Breach.

14.3.3. What District Data or PII was accessed, taken, or disclosed.

14.3.4. Who is responsible for the Security Breach and what factors caused or contributed to it.

14.3.5. What the Data Recipient has done or is doing to remediate adverse effects of the Security Breach.

14.3.6. What action or actions the Data Recipient has taken or is taking to prevent future Security Incidents and Security Breaches.

14.4. After a Security Breach has occurred, the District may take any one, all, or a combination of these actions:

14.4.1. Terminate the Contract.

14.4.2. Suspend performance under the Contract.

14.4.3. Stop the release of further District Data to the Data Recipient.

14.4.4. Disqualify the Data Recipient, its Subcontractors, or both, from future contracts with the District.

14.4.5. Take actions required or permitted by the Colorado Student Data Act, if applicable, and any other applicable law.

14.4.6. Avail itself of any other remedy available under the Contract and the law.

15. **Liability for Security Breach**. In addition to any other remedies available to the District under contract, law, or equity, the Data Recipient shall reimburse the District for all costs incurred by the District in the investigation and remediation of any Security Breach caused in whole or in part by the Data Recipient or the Data Recipient's Subcontractors, including but not limited to providing notification and credit monitoring services to affected individuals as required by law, the District, or both; and the payment of legal fees, audit costs, fines, and other fees and costs imposed against the District as a result of the Security Breach.

16. **Indemnification**. The Data Recipient indemnifies the District, holds the District harmless against, and shall defend the District against all claims, demands, suits, actions, and claims of any kind made by third parties against the District as the result of a Security incident, Security Breach, or other events arising out of or in any manner related to the DPA.

17. **Legal Orders and Discovery**.
    17.1. Directed to the Data Recipient. When the Data Recipient receives a Discovery Request, the Data Recipient shall:
        17.1.1. Promptly notify the District, except to the extent such notification is prohibited by law; and
        17.1.2. Consult with the District regarding its response to the Discovery Request; and
        17.1.3. Cooperate with the District's reasonable requests in connection with efforts by the District to respond to and deal with the Discovery Requests; and
        17.1.4. Provide the District with a copy of the Data Recipient's response to the Discovery Request.
    17.2. Directed to the District. When the District receives a Discovery Request seeking the District Data maintained by the Data Recipient, including but not limited to a request under the Colorado Open Records Act, and the District notifies the Data Recipient of the Discovery Request, the Data Recipient shall provide the requested District Data to the District within the time frame the District requires in the notification.
    17.3. Parent Requests.
        17.3.1. If a Student or their parent or legal guardian contacts the District with a request to review or correct District Data or PII, pursuant to FERPA or the Colorado Student Data Law or other laws, the District may notify the Data Recipient's Designated Representative. The Data Recipient shall then use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District, within 10 calendar days after receipt of the District's notice.

17.3.2. If a Student or their parent or legal guardian contacts the Data Recipient with a request to review or correct the District Data or PII, the Data Recipient shall promptly notify the District within 10 calendar days after the Data Recipient receives such contact and shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District.

18. **Click-Through Terms of Use**.
    18.1. Terms of Use. The Data Recipient's online-ordering process for Digital Services may require that the District, through its Schools, Departments, or End Users, agree to Terms of Use by Click-Through. If the District or an End User Clicks-Through the Terms of Use, and in addition to other provisions listed as *void ab initio* or deemed included elsewhere in the Contract, the following exceptions and conditions apply.
        18.1.1. If the duration of a License exceeds the duration of the Contract, then the terms of the Contract are automatically incorporated into the terms of License on the date when the Contract expires or otherwise terminates.
        18.1.2. Any provisions required by C.R.S. §22-1-135 are deemed to be included.
        18.1.3. The District **does not** consent to provisions that:
            18.1.3.1. Purport to limit the Data Recipient's liability.
            18.1.3.2. Remove ownership of District Data or De-identified Data or both from the District.
            18.1.3.3. Allow for use of District Data or De-identified Data outside of, in addition to, or in conflict with the Data Release Purpose.
            18.1.3.4. Provide for automatic renewal of any contractual obligation of the District.
            18.1.3.5. Impose confidentiality requirements on the District that conflict with the District's legal obligations, such as and without limitation, those regarding open records and government transparency.
            18.1.3.6. Waive District rights, including without limitation a waiver of jury trial or the shortening of the time period before limitations of action become effective.
            18.1.3.7. Are prohibited or void under C.R.S. §22-1-135. This includes, without limitation, provisions (i) requiring the District to indemnify others; (ii) requiring binding arbitration or other extra-judicial dispute resolution; (iii) waiving the Colorado Governmental Immunity Act; or (iv) conflicts with Colorado law. In the event of a conflict between this summary and C.R.S. §22-1-135, the statute governs.
    18.2. DPA Prevails. The terms of this DPA shall control in the event of an inconsistency or conflict between the DPA and the Terms of Use.

19. **Insurance**. The Data Recipient shall maintain policies of insurance to cover its liability that may arise under the DPA. In addition to any other insurance coverage that the Data

Recipient may carry, the Data Recipient shall maintain cyber insurance coverage with minimum coverage limits of $3,000,000 per occurrence and $5,000,000 in aggregate. The Data Recipient shall assume all financial responsibility for deductibles and self-insured retentions. At a minimum, the cyber insurance policy shall provide coverage for the following risks:

- Data breaches, including without limitation incidents involving theft of personal information.
- Cyber attacks on data held by the Data Recipient and its Subcontractors, vendors, and other third parties.
- Cyber attacks that occur anywhere in the world.
- Terrorist acts.

Insurance carriers providing coverage shall have an AM Best rating of A-VIII or better. The policies shall name the District an additional insured to the extent the insurance policy and carrier make naming additional insureds available. permits. On the District's request and where available, the insurance policy shall provide for waivers of subrogation. The Data Recipient shall require Subcontractors to maintain insurance policy coverages equivalent to and with coverage limits that are no less than those required of the Data Recipient in this DPA and shall in any event be sufficient to cover the Subcontractors' liability that may arise from their performance as Subcontractors. The Data Recipient shall provide evidence of insurance coverage upon the District's request. Certificates of insurance shall be in such form and substance sufficient to evidence that the insurance required under the Contract is in effect and shall provide information as to when insurance coverage expires. These requirements shall not be construed as a limitation of liability.

20. **Definitions**. As used in this DPA, the following terms have the following meaning.
    20.1. *"**Click-Through**"* means both (1) the act, by clicking or tapping on an electronic on-line or app button or link for that purpose, of accepting on-line terms and conditions, and (2) the resulting agreement between the Parties.
    20.2. ***"Colorado Student Data Law"*** means the Colorado Student Data Transparency and Security Act, C.R.S. § 22-16-101 *et seq.,* as amended from time to time.
    20.3. ***"Data Recipient"*** means the Person that is receiving District Data pursuant to the DPA and whose name is listed on the Cover Page.
    20.4. ***"Data Release Purpose"*** means the purpose or purposes for which the District provides District Data to the Data Recipient and is as stated on the Cover Page.
    20.5. "***De-identified Data***" means the District Data from which all PII, and attributes about District Data and PII, have been permanently and irrevocably removed so that no individual identification can be made.
    20.6. "***Designated Representative***" means the employee or other agent designated by each Party for their respective roles under the DPA to give and receive (i) Legal Notices, (ii) notices of Security Incidents and Security Breaches,

(iii) reports and other notices required by the DPA, and (iv) other information, and who may function as the coordinators to implement other aspects of the DPA as needed.

20.7. ***"Digital Services"*** means the internet websites, online services, online application, mobile application, website platforms, licensed software services, and other electronic and digital services that the Data Recipient or their Subcontractors may provide or use in accordance with the Data Release Purpose.

20.8. ***"Discovery Request"*** means any subpoena, warrant, legal process order, summons and complaint, interrogation, or other apparently or seemingly enforceable requirement from any jurisdiction seeking District Data.

20.9. ***"District"*** means the Jefferson County School The District R-1.

20.10. "***District Data"*** means:

20.10.1. PII, Records, and Education Records; and

20.10.2. Student PII as that term is defined by the Colorado Student Data Law; and

20.10.3. Data included therein or derived therefrom; and

20.10.4. Health, medical, financial, credit card, contract, and employment information about Students and their respective families, District employees and their respective families, and District suppliers, vendors, and contractors, that is protected by various State and federal laws applicable to the Contract; and

20.10.5. All data and metadata about District Data that the Data Recipient collects, generates, or infers; and

20.10.6. Data and information that the District makes available directly or indirectly to the Data Recipient; and

20.10.7. Data and information that the District **does not** also intentionally make or **has not** intentionally made generally available on public websites or publications.

20.10.8. Materials or content that Students and other District constituents create through use of Digital Services and that is delivered in connection with the Contract and includes, without limitation, essays, research reports, portfolios, music, audio files, photographs, videos, and account information.

20.10.9. With respect to Students only, data, 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, including without limitation:

20.10.9.1. The Student's name;

20.10.9.2. The name of the Student's parent or other family members;

20.10.9.3. The address or phone number of the Student or Student's family;

20.10.9.4. Personal identifiers such as the Student's state-assigned Student identifier, social security number, Student number or biometric record;

20.10.9.5. Indirect identifiers such as the Student's date of birth, place of birth, or mother's maiden name; and

20.10.9.6. Demographic attributes, such as race, socioeconomic information, and gender.

20.10.10. With respect to Students and all other individuals, and to the extent not already included in the above definition:

20.10.10.1. "Personal information" as defined in CORA; and

20.10.10.2. "Personally identifiable information" contained in Education Records;

20.10.10.3. "Protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103;

20.10.10.4. "Nonpublic personal information" as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809;

20.10.10.5. Credit and debit card numbers, PINs and other access codes, authentication data, and other cardholder data as those terms are defined in the Payment Card Industry Data Security Standards; and

20.10.10.6. Other financial account numbers, access codes, and state- or federal-identification numbers such as driver's license, passport or visa numbers.

20.11. ***"DPA"*** means this Data Protection Addendum.

20.12. "***Education Record***" means Records, files, documents and other materials that: (1) contain information directly related to a Student; and (2) are maintained by the District or by a Person acting for the District such as the Data Recipient.

20.13. "***End User***" means individuals authorized by the District to access and use the Digital Services.

20.14. ***"FERPA"*** means the federal Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. Part 99.

20.15. "***Mine District Data***" and all the conjugations of the verb "mine" means the act of searching through, analyzing, accessing, or extracting District Data, metadata, or information that is NOT necessary to accomplish, for the benefit of the District, the Data Release Purpose, the services contemplated under the Contract (if any), or other purpose or purposes of this DPA.

20.16. ***"Party"*** means either the District or the Data Recipient, and ***"Parties"*** means both the District and the Data Recipient.

20.17. ***"Person"*** means any individual, entity, including without limitation, any commercial, non-profit, governmental, or tribal organization, or other person of any kind that is not a Party.

20.18. "***Personally Identifiable Information***" or "***PII***" means any information that, alone or in combination, is linked or linkable to an individual so as to allow identification of this individual.

20.19. ***"Privacy Policy"*** means the document that the Data Recipient designates as its "Privacy Policy" and that sets forth the Data Recipient's practices and policies relating to data collection, use, protection, security, and disclosure.

20.20. "***Record***" means any information recorded in any way and on any medium, including, but not limited to, handwriting, print, computer or other digital media, video or audio tape, film, microfilm, and microfiche.

20.21. ***"School Service Contract Provider"*** means the same as defined in the Colorado Student Data Law.

20.22. "***Securely Destroy***" means to remove District Data from the Data Recipient's systems, paper files, Records, databases, and any other media regardless of format, in accordance with prevailing industry standards such as detailed in National Institute of Standards and Technology ("NIST") Guidelines for Media Sanitization, or such other standard to which the District may agree in writing, so that District Data is permanently irretrievable in the Data Recipient's and its Subcontractors' normal course of business.

20.23. "***Security Breach***" means an event where Unauthorized Activity has occurred.

20.24. ***"Security Incident"*** means a suspected, attempted, or imminent threat of Unauthorized Activity.

20.25. ***"Student"*** means any individual who is enrolled in or otherwise attending a District school, has at any time been enrolled in or attended a District school, or will at any time in the future be enrolled in or attending a District school.

20.26. ***"Student-Generated Content"*** means materials or content that a Student creates through use of Digital Services and includes, without limitation, essays, research reports, portfolios, music, audio files, photographs, videos, and account information.

20.27. ***"Student PII"*** means the same as defined in the Colorado Student Data Law.

20.28. "***Student Profile***" means a collection of PII data elements relating to a Student.

20.29. "***Subcontractor***" means any Person who assists the Data Recipient with the Data Release purpose pursuant to contractual arrangements between the Data Recipient and that Person, and with whom the District has no direct contractual relationship.

20.30. ***"Targeted Advertising"*** means the same as defined in the Colorado Student Data Law.

20.31. ***"Terms of Use"*** means the Data Recipient's or a Subcontractor's contractual terms and conditions for the access and use of Digital Services, such as, without limitations, the license terms, end user license agreement, and other terms of service, the consent to which is a condition of the Digital Service.

20.32. **"*Unauthorized Activity*"** means the illegal or otherwise unauthorized disclosure, release, acquisition, access to, alteration, use, disruption, or destruction of District Data, or a system configuration that results in a documented unsecured disclosure, access, alteration, or use that threatens, risks, or poses financial, reputational or other harm to the affected End User or the District.

Attachment 1 to DPA (Data Elements)

(To be completed if the Data Recipient is a School Service Contract Provider)

1. **The Data Recipient collects, generates or uses the following data elements of Student PII and other District Data**:

Data fields collected initially for account creation:

Data fields collected during application usage:

2. **The Data Recipient uses District Data for the following learning or educational purposes**: To provide the educational tools and curriculum per the Contract.

3. **The Data Recipient uses and shares the Student PII and other District Data as follows:**

As governed by applicable law, only in accordance with the terms of the Contract, and only as necessary for the Data Release Purpose.