Weld County School District 6
Data Protection Agreement

This Data Protection Agreement is attached to and forms a part of the Quote dated May 2018, by and between Weld County School District 6 ("District") and College Board ("Vendor"). This Agreement supersedes the Contract by adding to, deleting from and modifying the Contract as set forth herein. To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Contract and this Agreement, this Agreement shall govern and the terms of the Contract that conflict with this Agreement or are inconsistent with this Agreement shall be of no force or effect.

1. Definitions

a. "Anonymized Data" means De-identified Data, as defined below, which does not include a record code and cannot be linked to the original data source.

b. "Authorized Persons" means Vendor's employees or subcontractors who have a need to know and will access District Data to enable Vendor to perform its obligations under this Agreement.

c. "De-identification" means the process of removing or obscuring all identifiable information until all data that can lead to individual identification has been expunged or masked. Simple removal of direct identifiers from data does not constitute adequate de-identification. District Data that has undergone sufficient De-identification shall be referred to as De-identified Data.

d. "District Data" means information, including, but not limited to, Personally Identifiable Information, business, administrative and financial information, intellectual property information, and other information that is not intentionally made generally available by the District on public websites or publications, that is provided to Vendor by or at the direction of District in the course of Vendor's performance under this Agreement. "District Data" includes metadata and data derived from the use of District Data and metadata.

e. "End User" means the individuals authorized by the District to access and use the Services provided by the Vendor under this Agreement.

f. "Personally Identifiable Information" or "PII" shall mean District Data that, alone or in combination, is linked or linkable to a specific student or person that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student or person with reasonable certainty. PII includes, but is not limited to, a student's name; the name of a student's parent; guardian or other family member; the address of a student or a student's family; a personal identifier such as a student's social security number, student number, or biometric record; other indirect student identifiers such as a student's date of birth, place of birth, or mother's maiden name; and various demographic attributes, such as race, socioeconomic information, and gender. To the extent it is not already included in the definition hereinabove, PII also includes "personal information" as defined in the Colorado Open Records Act, C.R.S. 24-72-101 *et seq*.; personally identifiable information contained in student "education records" as that term is defined in the Family Educational

Rights and Privacy Act, 20 U.S.C. 1232g; "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; "nonpublic personal information" as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, and state- or federal-identification numbers such as driver's license, passport or visa numbers.

g. "Securely Destroy" means taking actions that render data written on physical or electronic media unrecoverable by both ordinary and extraordinary means.

h. "Security Breach" means an event in which District Data is exposed to unauthorized disclosure, access, alteration or use or a system configuration that results in unsecured disclosure, access, alteration or use, such as a failed firewall or password disclosure.

i. "Services" means any good or services acquired by the District from the Vendor, including, but not limited to, computer software, mobile applications (apps), and web-based tools accessed by students and/or their parents through the Internet or on a hard drive of a computer or electronic device and used for educational purposes.

j. "Mining District Data" means to search through, analyze, access, or extract District Data, metadata, or information that is not necessary to accomplish the Services or purpose(s) of this Agreement for the benefit of the District.

2. Rights and License in and to District Data

District retains all right, title, and interest in and to the District Data, including without limitation all now known or hereafter existing rights associated with works of authorship, including copyrights and moral rights; trademarks or service mark rights; trade secret rights; patents and patent rights; and all other intellectual property (collectively referred to as "Intellectual Property"). For the term of this Agreement, unless sooner terminated, Vendor shall have a limited, nonexclusive license to use the District Data and Intellectual Property solely for the purpose of performing its obligations hereunder. This Agreement does not give Vendor any rights, title, or interest, implied or otherwise, to District Data or Intellectual Property, except as expressly stated in the Agreement. District shall have the right to access and retrieve District Data stored by or in possession of Vendor at any time upon written notice to Vendor.

3. Data Privacy

a. Vendor will use District Data only for the purpose of performing the Services and fulfilling its duties under this Addendum and will not use, sell, rent, transfer, distribute, alter, mine, or disclose such data, including Anonymized Data, to any third party without the prior written consent of the District, except as required by law. If District consents in writing to Vendor's use of Anonymized Data, then Vendor agrees not to attempt to re-identify the Anonymized Data.

b. District Data will not be stored outside the continental United States unless Vendor has given the District advance written notice of where and how the servers are housed and managed and the District has consented in writing to such storage.

c. Vendor will provide access to District Data, including De-identified Data, only to its Authorized Persons. Vendor will ensure that all Authorized Persons have received and understood appropriate instruction as to how to comply with the data protection provisions of this Agreement. Upon District's written request, Vendor shall promptly identify in writing all Authorized Persons as of the date of such request. Vendor shall at all times cause such Authorized Persons to abide strictly by Vendor's obligations under this Agreement. Vendor further agrees to maintain a disciplinary process, up to and including termination, to address any unauthorized use, modification or disclosure of District Data by any Authorized Persons.

e. Vendor warrants and represents that during the five-year period preceding the Effective Date of the Agreement, it has not been found in violation of FERPA by the Family Policy Compliance Office.

f. With the exception of De-identified Data that the District has agreed in writing to allow Vendor to use, Vendor will not use District Data for its own commercial benefit, including but not limited to, advertising or marketing purposes, unless such use is specifically authorized by this Agreement or otherwise authorized in writing by the District.

g. In performance of the Services required by the Agreement, Vendor may collect personal information (as defined in the Children's Online Privacy and Protection Act of 1998, 5 U.S.C. 6501 to 6505 and its implementing regulations) from children under thirteen years of age. Vendor warrants, represents, and covenants that such collection is and shall be for the use and benefit of the District and for no other commercial purpose. Vendor has provided District with full notice of its collection, use, and disclosure practices.

h. Vendor is prohibited from building a personal profile of a student or Mining District Data for any purposes other than those agreed to by the Parties; provided, however, Vendor is not prohibited from using District Data for purposes of adaptive learning or customized education when used solely for the purpose of performing the Services or its obligations hereunder.

i. Upon District's written request, to confirm Vendor's compliance with this Agreement and/or any applicable laws, regulations, and/or industry standards, Vendor shall provide District with the most recent copy of the Vendor's network security audit.

4. Data Security

a. Vendor will store and process District Data in accordance with commercial best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in FIPS PUB 200, to secure such data from unauthorized access, disclosure, alteration, and use. Vendor shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with all applicable

federal and state data protection and privacy laws, regulations and directives, as well as the terms and conditions of this Addendum. Without limiting the foregoing, and unless expressly agreed to the contrary in writing, Vendor warrants that all electronic District Data will be:

i. encrypted at 128-bit level in transmission using SSL (Secure Sockets Layer) and

ii. stored at no less than 128-bit level encryption.

b. Upon request, Vendor will provide District certification indicating that an independent vulnerability or risk assessment of the Vendor's data security program has occurred.

5. Security Breach

a. *Response.* Immediately upon becoming aware of a Security Breach, a complaint of a Security Breach or of circumstances that could have resulted in unauthorized access to or disclosure or use of District Data, Vendor will notify the District in writing, fully investigate the incident, cooperate fully with the District's investigation of and response to the incident, and use best efforts to prevent any further Security Breach at Vendor's expense in accordance with applicable privacy laws. Except as otherwise required by law, Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the District.

b. *Liability*. In addition to any other remedies available to the District under law or equity, Vendor will reimburse the District in full for all costs incurred by the District in investigation and remediation of any Security Breach caused in whole or in part by Vendor or Vendor's Authorized Persons, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed against the District as a result of the Security Breach.

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

a. Except as otherwise expressly prohibited by law, Vendor will immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking District Data; consult with the District regarding its response; cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and, upon the District's request, provide the District with a copy of its response.

b. If the District receives a subpoena, warrant, or other legal order, demand (including any request pursuant to the Colorado Open Records Act) or request seeking District Data maintained by Vendor, the District will promptly notify Vendor and Vendor will promptly supply the District with copies of the District Data for the District to respond.

c. Vendor agrees to fully cooperate, at its own expense, with District in any third party litigation or other formal action the District reasonably deems necessary to protect its rights relating to the use, disclosure, protection and maintenance of District Data as required under applicable law.

7. Data Transfer Upon Termination or Expiration

With the exception of De-identified District Data that District has specifically agreed in writing to allow Vendor to use after termination or expiration of the Agreement, upon termination or expiration of the Agreement, Vendor will ensure that all District Data is securely returned or destroyed as directed by the District. Transfer to the District or a third party designated by the District shall occur within a reasonable period of time but no later than thirty (30) days after expiration or termination of the Agreement, and without significant interruption in service or access. Vendor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. In the event that the District requests destruction of its data, Vendor agrees to Securely Destroy all data in its possession and in the possession of any Authorized Persons to which the Vendor might have transferred District Data. The Vendor agrees to promptly certify in writing to District that such District Data has been returned to District or disposed of securely.

8. Audits

The District reserves the right in its sole discretion to perform audits of Vendor at the District's expense to ensure compliance with the terms of this Agreement and all applicable laws, regulations, and industry standards. The Vendor shall reasonably cooperate in the performance of such audits.

9. No End User Agreements

This Agreement is the entire agreement between the District (including End Users) and the Vendor. In the event that the Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with End Users, the parties agree that in the event of a conflict between the terms of any such agreement and this Agreement, the terms of this Addendum and the Contract, in that order of precedence, shall control.

10. Transparency

Within ten (10) business days after signing this Agreement, to the extent not previously provided, Vendor shall make available to District the following information about its products or services, as applicable: (a) type of PII that is collected or generated by the Vendor or disclosed to a third party; (b) the educational purpose for which the PII is used; (c) Vendor's policies regarding retention and disposal of PII; and (d) type of information, including but not limited to PII, that is collected and how it is shared or used. In addition, Vendor shall notify District prior to changing its privacy policies and shall cooperate with any students or parents who request a reasonable correction of student information created or maintained by Vendor.

11. School Service Contract Provider

If Vendor is a "school service contract provider" as defined in the Colorado Student Data Transparency and Security Act, C.R.S. §§ 22-16-101 to -112, then Vendor shall comply with the requirements set forth in C.R.S. §§ 22-16-108, -109, and -110.

12. Termination

Subject to Section 15, this Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Contract between the Parties.

13. Indemnification

Vendor shall indemnify and hold District and its directors, employees, board members and agents from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, award, penalties, fines, costs or expenses, including attorneys' fees, the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against District or its directors, employees, board members and agents arising out of or resulting from Vendor's failure to comply with any of its obligations under this Addendum. These indemnification duties shall survive termination or expiration of the Agreement.

14. Insurance

Vendor shall purchase and maintain during the term of this Agreement Technology Errors and Omissions/Professional Liability Insurance, including Network Security and Privacy Liability Insurance. Such policy shall cover professional misconduct or lack of ordinary skill in providing services, systems and/or product as defined in the scope of services of this Agreement. In the event that the professional liability insurance required by this Agreement is written on a claims-made basis, Vendor warrants that any retroactive date under the policy shall precede the effective date of this Agreement; and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of two (2) years beginning at the time work under this Agreement is completed. If such insurance is maintained on an occurrence form basis, Vendor shall maintain such insurance for an additional period of one (1) year following termination of Agreement. If such insurance is maintained on a claims-made basis, Vendor shall maintain such insurance for an additional period of three (3) years following termination of the Agreement. If Vendor contends that any of the insurance it maintains pursuant to other sections of this clause satisfies this requirement (or otherwise insures the risks described in this section), then Vendor shall provide proof of same. The insurance shall provide coverage for the following risks:

a. Any error, misstatement, misleading statement, act, omission, neglect, breach of duty or personal injury offense for the Vendor rendering or failure to render technology services and the failure of the Vendor's technology products to perform the function or serve the purpose intended.

b. Liability arising from theft, dissemination and/or use of District Data stored or transmitted in electronic form.

c. Network Security Liability arising from the unauthorized access to, use of or tampering with computer systems including hacker attacks, inability of an authorized third party, to gain access to Vendor's services including denial of service, unless caused by a mechanical or electrical failure.

d. Liability arising from the introduction of a computer virus into, or otherwise causing damage to, a customer's or third person's computer, computer system, network or similar computer related property and the data, software, and programs thereon.

In addition to the foregoing requirements, the policy shall provide a waiver of subrogation in favor of the District and shall be endorsed to include the following additional insured language: "Weld County School District 6, and its elected officials, trustees, employees, and agents, shall be named as additional insureds with respect to liability arising out of the activities performed by, or on behalf of the Vendor." The policy shall be for the following amounts:

For Agreements of $500,000 or less		
Minimum Limits:		
Per Loss	$	1,000,000
Aggregate	$	3,000,000
For Agreements over $500,000		
Minimum Limits:		
Per Loss	$	3,000,000
Aggregate	$	5,000,000

15. Survival

The Vendor's obligations under Sections 3, 4, 5, 7, 8, 11, 13, and 14 shall survive termination of the Agreement until all District Data has been returned or Securely Destroyed.

[Signature page appears on next page]

IN WITNESS WHEREOF, the parties have executed this Addendum contemporaneously with the Contract.

WELD COUNTY SCHOOL DISTRICT 6	VENDOR
By: Mandy Hydock, Director of Finance	By: College Board
	Legal Name of Vendor
Date: Jun 27, 2018	13-1623965
	FEIN
	DocuSigned by: Trevor Packer C2E7EBB677DF4CC...
	Signature of Authorized Officer
	Senior Vice President AP & College Readiness Advanced Placement
	Title of Authorized Officer
	Date: 06/26/2018

4848-8959-8764, v. 1