DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

Weld County School District 6
Data Protection Agreement

This Data Protection Agreement is attached to and forms a part of the Discovery Education agreement dated July 10, 2018, by and between Weld County School District 6 ("District") and Discovery Education ("Vendor"). This Agreement is in addition to 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. This Agreement, having been drafted by the District will be interpreted with prejudice against the drafter.

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, subcontractors, or agents 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.

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

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, or if an End User gives the Vendor rights, title, or interest in the their data. District shall have the right to request the deletion of District Data stored by or in possession of Vendor at any time upon written notice to Vendor with the understanding certain requests might make the Vendor's Services to the District inoperable.

3. Data Privacy

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

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. Vendor may use Anonymized Data and including metadata for analysis and improvement of its products. 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.

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. 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.

d. Vendor states 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.

e. 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.

f. 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.

g. 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, customized education, and/or product enhancements when used solely for the purpose of performing the Services or its obligations hereunder.

h. 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 industry standards and according to Vendor's Data Security Policy, attached here as Exhibit 1, including implementing

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

appropriate administrative, physical, and technical safeguards, 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.* Upon becoming aware of a Security Breach, Vendor will notify the District in writing, fully investigate the incident, cooperate 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. When necessary and if possible in coordination with the District, Vendor will 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 reasonable direct out-of-pocket third party costs incurred by the District specifically remediating any Security Breach caused by Vendor or Vendor's Authorized Persons.

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

a. Except as otherwise expressly prohibited by law, Vendor will promptly notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking District Data and reasonably 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.

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.

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 destroyed. Vendor agrees to Securely

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

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 upon written request from the District to certify in writing to District that such District Data has been disposed of securely.

8. Audits

The District may annually perform an audit of Vendor's records specifically and directly related to the Services under this Agreement at the District's expense at the Vendor's principal place of business during normal business hours 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.. Transparency

Upon written request from the District to the Vendor 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 cooperate with any students or parents who request a reasonable correction of student information under the Services created or maintained by Vendor.

10. 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.

11. Termination

Subject to Section 14, this Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Contract between the Parties.

12. Indemnification

Vendor shall indemnify and hold District and its directors, employees, board members and agents from and against all losses, damages, actions, judgments, award, penalties, fines, reasonable out-of-pocket costs or expenses, including reasonable out-of-pocket attorneys' fees, 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 negligence or failure to comply with any of its material obligations under this Addendum. These indemnification duties shall survive termination or expiration of the Agreement.

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

13. 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. 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

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

14. Survival

The Vendor's obligations under Sections 3, 4, 5, 7, 8, 10, 12, and 13 shall survive termination of the Agreement until all District Data has been Securely Destroyed.

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

WELD COUNTY SCHOOL DISTRICT 6

By: Mandy Hydock, Director of Finance

Date: Aug 10, 2018

VENDOR

By: Discovery Education

Legal Name of Vendor

36-2298050

FEIN

DocuSigned by:

F5DDC890367B42F...

Signature of Authorized Officer

President, K-12 Education

Title of Authorized Officer

Date: _____

4848-8959-8764, v. 1

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

EXHIBIT 1

DISCOVERY EDUCATION, INC. DATA SECURITY POLICY

This Policy describes, in general, (i) what steps Discovery Education, Inc. ("Discovery") takes to protect personally identifiable information ("PII") that is provided to Discovery; (ii) how PII may be used; (iii) with whom Discovery may share PII, and (iv) the steps Discovery takes to protect the PII.

No student PII is required for the use of any of the basic Discovery Education services, however, in the event Users elect to use any of the functionality within the Discovery Education services which provide personalized pages, individual accounts, other user-specific customization, or otherwise submit or upload information (all such data is generally limited to the following: school name, first name, last name, and grade level), all such PII provided to Discovery will be protected in accordance with this Policy.

No school employee PII is required for Professional Development Services other than first name and last name for the purposes of attendance logs.

I. DEFINITIONS

Capitalized terms referenced herein but not otherwise defined shall have the meanings as set forth below:

"Authorized Disclosee" means the following: (1) third parties to whom the Subscriber/Customer/Distributor has given Discovery written approval to disclose PII; (2) third parties to whom disclosure is required by law; and (3) if applicable, third party vendors working on Discovery's behalf or performing duties in connection with Discovery's services (e.g. hosting companies) to whom Subscriber/Customer/Distributor herein gives Discovery written approval to disclose PII received from Subscriber/Customer/Distributor and its Users and who are required to implement administrative, physical, and technical infrastructure and procedural safeguards in accordance with accepted industry standards.

"Authorized User" means a Discovery employee authorized by the Subscriber/Customer/Distributor to access PII in order to perform services under an Agreement.

"Destroy" or "Destruction" means the act of ensuring the PII cannot be reused or reconstituted in a format which could be used as originally intended and that the PII is virtually impossible to recover or is prohibitively expensive to reconstitute in its original format.

"FERPA" means the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S.C. § 1232g) and its implementing regulations, as they may be amended from time to time. The regulations are issued by the U.S Department of Education, and are available at http://www2.ed.gov/policy/gen/reg/ferpa/index.html.

"Personally Identifiable Information" (or "PII") means any information defined as personally identifiable information under FERPA.

II. PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION

Basic Privacy Protections

1. Compliance with Law and Policy. All PII provided to Discovery is handled, processed, stored, transmitted and protected by Discovery in accordance with all applicable federal data privacy and security laws (including FERPA) and with this Policy.

2. Training. Employees (including temporary and contract employees) of Discovery are educated and trained on the proper uses and disclosures of PII and the importance of information privacy and security.

3. Personnel Guidelines. All Discovery employees are required to be aware of and work to protect the confidentiality, privacy, and security of PII. Discovery, and its respective personnel do not access PII except to

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

comply with a legal obligation under federal or state law, regulation, subpoena, or if there is legitimate need for the information to maintain data systems or to perform required services under the Agreement with Subscriber/Customer/Distributor. The following provides a general description of the internal policies to which Discovery and its respective personnel adhere:

a. Limit internal access to PII to Discovery personnel with proper authorization and allow use and/or disclosure internally, when necessary, solely to personnel with a legitimate need for the PII to carry out the services provided under the Agreement.
b. Disclose PII only to Authorized Disclosees.
c. Access PII only by Authorized Users.
d. When PII is no longer needed, delete access to PII.
e. Permit employees to store or download information onto a local or encrypted portable devices or storage only when necessary, and to create a written record for retention verifying that the information is encrypted and stored in password-protected files, and that devices containing the information have appropriate security settings in place (such as encryption, firewall protection, anti-virus software and malware protection).
f. Any downloaded materials consisting of PII remain in the United States.
g. Prohibit the unencrypted transmission of information, or any other source of PII, wirelessly or across a public network to any third party.
h. Upon expiration or termination of Agreement, Discovery shall Destroy all PII previously received from Subscriber/Customer/Distributor no later than sixty (60) days following such termination, unless a reasonable written request is submitted by Subscriber/Customer/Distributor to Discovery to hold such PII. Each electronic file containing PII provided by Subscriber/Customer/Distributor to Discovery will be securely Destroyed. This provision shall apply to PII that is in the possession of Discovery, Discovery employees/personnel and/or Authorized Disclosees.

Information Security Risk Assessment

Discovery periodically conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic, paper, or other records containing PII maintained by Discovery; Discovery reports such risks as promptly as possible to Subscribers/Customers/Distributors; and Discovery implements security measures sufficient to reduce identified risks and vulnerabilities. Such measures are implemented by Discovery based on the level of risks, capabilities, and operating requirements. These measures include, as appropriate and reasonable, the following safeguards:

1. Administrative Safeguards

a. Sanctions: Appropriate sanctions against Contractor personnel who fail to comply with Discovery's security policies and procedures.
b. System Monitoring: Procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.
c. Security Oversight: Assignment of one or more appropriate management level employees of Discovery to be responsible for developing, implementing, and monitoring of safeguards and security issues.
d. Appropriate Access: Procedures to determine that the access of Discovery personnel to PII is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Discovery personnel who have access to PII.
e. Employee Supervision: Procedures for regularly monitoring and supervising Discovery personnel who have access to PII.
f. Access Termination: Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.

2. Physical Safeguards

a. Access to PII: Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.
b. Awareness Training: On-going security awareness through training or other means that provide Discovery personnel (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training also addresses procedures for monitoring log-in attempts and reporting discrepancies, as well as procedures for safeguarding passwords.

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

c. Incident Response Plan: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.
d. Physical Access: Procedures to limit physical access to PII and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed, including physical barriers that require electronic control validation (e.g., card access systems) or validation by human security personnel.
e. Physical Identification Validation: Access is physically safeguarded to prevent tampering and theft, including procedures to address control and validation of a person's access to facilities based on his or her need for access to the PII.
f. Operational Environment: Procedures that specify the proper functions to be performed, the manner in which they are to be performed, and the physical attributes of the surroundings of facilities where PII is stored.
g. Media Movement: Procedures that govern the receipt and removal of hardware and electronic media that contain PII into and out of a facility.

3. Technical Safeguards

a. Data Transmissions: Technical safeguards, including encryption, to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups.
b. Data Integrity: Procedures that protect PII maintained by Discovery from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.
c. Logging off Inactive Users: Inactive electronic sessions are designed to terminate automatically after a specified period of time.
d. Data Backup: Data is backed up daily and stored offsite for thirty days. In the event data has to be restored, data backups can be retrieved from offsite locations in one business day and the process of restoration would take an additional day.
e. Disaster Recovery: Disaster Recovery procedures are in place and are tested on a yearly basis. Discovery has two datacenters located in the United States that are utilized to recover operations.

Security Controls Implementation

Discovery has procedures addressing the acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the need for management and staff to understand their responsibilities and have the knowledge, skills and motivation necessary to fulfill their duties.

Security Monitoring

In combination with periodic security risk assessments, Discovery uses a variety of approaches and technologies to make sure that risks and incidents are appropriately detected, assessed and mitigated on an ongoing basis. Discovery also assesses on an ongoing basis whether controls are effective and perform as intended, including intrusion monitoring and data loss prevention.

Security Process Improvement

Based on Discovery's security risk assessments and ongoing security monitoring, Discovery gathers and analyzes information regarding new threats and vulnerabilities, actual data attacks, and new opportunities for managing security risks and incidents. Discovery uses this information to update and improve its risk assessment strategy and control processes.

Audit

Discovery acknowledges Subscriber's/Customer's/Distributor's right to audit any PII collected by Discovery and/or the security processes listed herein upon reasonable prior written notice to Discovery's principal place of business, during normal business hours, and no more than once per year. Discovery shall maintain records and documentation directly and specifically related to the services performed under the Agreement for a period of three (3) years, unless otherwise stated in Section II (3)(h) of this Policy.

Breach Remediation

DocuSign Envelope ID: B140DB1D-2895-4914-9184-F79776B8A05A

Discovery keeps PII provided to Discovery secure and uses reasonable administrative, technical, and physical safeguards to do so. Discovery maintains and updates incident response plans that establish procedures in the event a breach occurs. Discovery also identifies individuals responsible for implementing incident response plans should a breach should occur.

If a Subscriber/Customer/Distributor or Discovery determines that a breach has occurred, when there is a reasonable risk of identity theft or other harm, or where otherwise required by law, Discovery provides any legally required notification to affected parties as promptly as possible, and fully cooperates as needed to ensure compliance with all breach of confidentiality laws.

Discovery reports as promptly as possible to Subscribers/Customers/Distributors (or their designees) and persons responsible for managing their respective organization's incident response plan any incident or threatened incident involving unauthorized access to or acquisition of PII of which they become aware. Such incidents include any breach or hacking of Discovery's Electronic Data System or any loss or theft of data, other electronic storage, or paper. As used herein, "Electronic Data System" means all information processing and communications hardware and software employed in Discovery's business, whether or not owned by Discovery or operated by its employees or agents in performing work for Discovery.

Personnel Security Policy Overview

Discovery mitigates risks by:

1. Performing appropriate background checks and screening of new personnel, in particular those who have access to PII.
2. Obtaining agreements from internal users covering confidentiality, nondisclosure and authorized use of PII.
3. Providing training to support awareness and policy compliance for new hires and annually for personnel.