



Amendment No. 1 To Discovery Education, Inc. Boces Purchase Contract

WHEREAS, an Agreement was made between the Board of Cooperative Educational Services for the Monroe 1 County BOCES (the "BOCES") attached hereto as Exhibit A, and Discovery Education, Inc. ("Discovery") dated December 2, 2020 concerning the arrangement between BOCES and Discovery; and

WHEREAS, the Agreement, as amended, expires on June 30, 2025; and

WHEREAS, such amendment is permitted under New York State and local laws.

NOW, THEREFORE, the parties mutually agree to the following:

The optional pricing for License, Professional Development and Mystery Science Membership fees for the 2022/2025 school year shall be as follows:

Discovery Education BOCES Services and Pricing

The Fees payable by Distributor to Discovery for each school's subscription Package shall be calculated on a per-school basis as set forth below:

Service	Discovery List Rates	22 - 23 BOCES	23 - 24 BOCES	24 - 25 BOCES
DE streaming K-8	N/A	\$1,550	\$1,650	N/A
DE streaming K-12 or 9-12	N/A	\$1,935	\$1,985	N/A
Per Student Option (only available for district-wide purchase)	N/A	\$3.10	\$3.30	N/A
DE.X Upgrade	\$1,850	\$850	\$800	N/A
DE.X Upgrade Per Student Option (only available for district wide purchase)	N/A	\$1.90	\$2.00	N/A
Discovery Education Experience K-8	\$4,000	\$2,400	\$2,450	\$2,500
Discovery Education Experience K-12 or 9-12	\$4,000	\$2,785	\$2,785	\$2,785
Per Student Option (only available for district wide purchase)		\$5.00	\$5.30	\$5.55
STEM Connect (discount for current DE.X Schools Only)	\$3,000	\$2,700	\$2,700	\$2,700
DE Science K8	\$1,995	\$1,695	\$1,695	\$1,695
Professional Development	\$3,000	\$3,000	\$3,000	\$3,000

On site PD Session (One 6-hour session for up to 25 participants)				
Virtual Hourly Professional Development: 4 Hours	\$3,000	\$2,000	\$2,000	\$2,000
Virtual Hourly Professional Development: 48 Hours + 4 hours free = 52 hours	\$22,000	\$22,000	\$22,000	\$22,000
Science Techbook K-8 (National/Classic)	\$11.50	\$10	\$10	\$10
Science Techbook 9-12 (National/Classic)	\$11.50	\$10	\$10	\$10
Science Techbook Middle School (Modular) - site	\$7,000	\$6,025	\$6,025	\$6,025

Science Techbook Middle School (Modular) - student	\$18	\$15.5	\$15.5	\$15.5
--	------	--------	--------	--------

Social Studies Techbook 6-8	\$11.50	\$10	\$10	\$10
Social Studies Techbook 9-12	\$11.50	\$10	\$10	\$10
Math Techbook 6-8	\$11.50	\$10	\$10	\$10
Math Techbook 9-12	\$11.50	\$10	\$10	\$10
Bundles Math (6-8), Science (National K-5)- per site	\$9,500	\$6,900	\$6,950	\$7,000
Bundles, Math (9-12) Science (Classic 9-12)- per site	\$9,500	\$7,285	\$7,285	\$7,285
Bundles Math, Science (National/Classic)- per student	\$20	\$15	\$15	\$15
Bundles Social Studies- per site	\$9,500	\$5,810	\$5,860	\$5,910
Additional TB bundle site Math, Science (National/Classic)	\$5,500	\$4,500	\$4,500	\$4,500
Additional TB bundle site Social Studies	\$5,500	\$4,500	\$4,500	\$4,500
Science Techbook Middle School (Modular) Bundle - per site	\$11,000	\$8,250	\$8,250	\$8,250
Science Techbook Middle School (Modular) Bundle - student	\$24	\$18	\$18	\$18

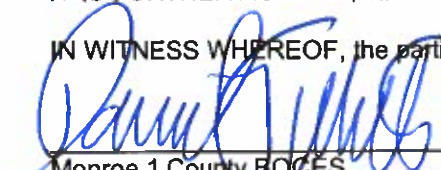
Print		Current Discovery Education listed rates	Current Discovery Education listed rates	Current Discovery Education listed rates
Kits		Current Discovery Education listed rates	Current Discovery Education listed rates	Current Discovery Education listed rates

Mystery Science Membership				
Standard (200+ students) Per building cost	\$1,999	\$1,125	\$1,125	\$1,125
Small School (100 - 199 students) Per building cost	\$849	\$725	\$725	\$725

Microschool (1 - 99 students) Per building cost	\$349	\$299	\$299	\$299
Grades K - 1 Pack (Requires Pack Shipping)	\$265	\$265	TBD	TBD
Grades 2 - 5 Pack (Requires Pack Shipping)	\$365	\$365	TBD	TBD
Pack Shipping (Requires Pack Shipping)	\$35	\$35	TBD	TBD

IT IS FURTHER AGREED, all other terms of the Agreement shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Amendment No. 1 as of the last signature date written below.



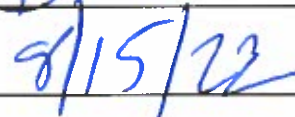
Monroe 1 County BOCES



Print Name



Title



Date

DocuSigned by:

78B6C33846A8450

Discovery Education, Inc.

Travis Barrs

Print Name

Head of Global Operations

Title
July 1, 2022

Date





BOCES PURCHASE CONTRACT

Region: MONROE 1 CO BOCES (M1 BOCES) (the "BOCES") Address: 41 OCONNOR RD FAIRPORT, NY 14450 - 1327 United States	Signature: _____ Name: _____ Title: _____ Date: <u>12/2/2020</u>
---	---

This **BOCES Purchase Contract** (the "Contract") is made as of 11/17/2020 by and between the **BOCES ("BOCES")** and **Discovery Education, Inc. ("Discovery")**. Discovery hereby grants to the **BOCES** the non-exclusive non-transferable right, during the Term, to purchase Licenses to Discovery Education Services for public schools located in the Community.

Licenses: up to four (4) year license to access the Discovery Education Services.

Term: 07/01/2020 through 06/30/2022, with renewal option to extend the pricing below for two additional years for individual schools and districts via the **BOCES** if certain requirements in the Purchase, Rate, and Downgrade Terms section are met. This Contract is subject to termination at any time for any reason upon thirty (30) days' notice.

Community: public schools located in the school districts located in the **BOCES'** service area and within the State of New York.

Discovery Education Services and Pricing:
(all pricing per school per year unless noted)

Discovery Education Streaming™: (includes extensions of existing Licenses)		
	<u>2020-2021</u>	<u>2021-2022</u>
K-8	\$1,450.00	\$1,475.00
K-12 / 9-12	\$1,895.00	\$1,905.00
Per student option	\$2.90	\$2.95
(per student per year, available only for district-wide purchase.)	unless locked in based on terms below.	
Optional add-on products and services:		
DEX Upgrade	\$880.00	\$880.00
Per student option	\$1.60	\$1.60
DEX per student upgrade (per student per year, available only for district-wide purchase)		
Discovery Education Experience:		
K-8	\$2,330.00	\$2,355.00
K-12 / 9-12	\$2,775.00	\$2,785.00
Per student option	\$4.50	\$4.55
(per student per year, available only for district-wide purchase)		
Discovery Education Coding (requires DE.X service):		
K-8	\$ 500.00	\$ 500.00
Discovery Education Science:		
K-8	\$1,695.00	\$1,695.00
Discovery Education Health: \$1,425.00 \$1,425.00		
STEM Connect (requires DE.X service):		
	\$2,700.00	\$2,700.00
Professional Learning (On site PD Session, One 6-hour session for up to 25 participants)		
DE.X Professional Development Launch Bundle (3 Days)	\$8,500.00	\$8,500.00
On-Site Product Training Session	\$2,500.00	\$2,500.00
On-Site Professional Learning Session	\$3,000.00	\$3,000.00

Price Adjustments: Fees for initial Licenses of less than one year will be prorated, based on number of complete calendar months in the term of such License.

Order Placement: The **BOCES** may add schools to this Contract by providing a "School Notice" to Discovery, which may be in the form of a purchase order. Upon receipt of a School Notice, the schools referenced therein shall be added to this Contract and their Licenses shall become effective. School Notices must include the information below: Name of applicable district, Name and address of each school, Grade level of each school, Student enrollment in each school, Start and end date of license term. Schools may also be removed at any time and without additional expense upon notice by **BOCES**.

Payment: Due and payable within 30 days of Discovery's receipt of a School Notice.

BOCES Fees: The **BOCES** will have the right to charge each subscribing school in its service Public area a fee for the License.

Additional Terms and Conditions

BOCES Obligations: In consideration for the **BOCES Fees**, the **BOCES** agrees to the following obligations:

- Ensure subscribing schools agree to comply with the Standard Terms of Service and License located at <https://www.discoveryeducation.com/terms-of-use>.
- Make available information regarding Discovery Education Services to schools in the Community, using **BOCES** created materials or materials provided by Discovery for such purpose.
- Use reasonable effort to provide two 1/2 day user group trainings for Discovery Education Services to school district personnel in the Community.
- Allow Discovery to present to districts at least twice a year at a **BOCES** location, if practicable.
- Provide basic customer support.

Confidentiality: All provisions of this Contract ("Confidential Information") shall be kept strictly confidential by the parties and may not be disclosed without request via the Freedom of Information Law (FOIL). In the event that **BOCES** receives a FOIL request for Confidential Information, **BOCES** shall immediately notify Discovery of such request and forward a copy of such request to Discovery, attn: Legal Department. **BOCES** shall, upon receipt of any such request for disclosure of Confidential Information, use its best efforts to contest the disclosure of Confidential Information under all exceptions and/or exemptions, if any, that are applicable to such Confidential Information under FOIL.

Miscellaneous: Discovery may revise the Terms of Use from time to time and shall use reasonable efforts to notify the **BOCES** of such changes. This Contract contains the entire understanding and supersedes all prior understandings between the parties relating to the subject matter herein. Signatures exchanged by facsimile or electronically by PDF shall have the same binding effect as original signatures.

Data Security and New York Education Law § 2-d Compliance:
While **BOCES** on behalf of itself and those schools in the Community acknowledge that no student personal information is required for the use of any of the basic Discovery Education services, in the event those schools in the Community or their 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 (such data generally limited to first name, last name, grade level and school name), **BOCES** on behalf of itself and those schools in the Community represent and warrant that to the best of its knowledge those schools in the Community have all necessary authorization to provide to Discovery any information it provides through Discovery services in order to use such functions. Consent is required for the collection, use and disclosure of personal information obtained from children through certain online services, and to the extent required, **BOCES** on behalf of itself and those schools in the Community consent to Discovery's use of such information in the course of providing the Discovery Education services. Discovery agrees to maintain and/or use any student personal information and data provided to it by those schools in the Community or their users only in compliance with (i) the Children's Online Privacy Protection Act of 1988 ("COPPA"), (ii) the Family Educational Rights & Privacy Act of 1974 ("FERPA"), (iii) the Children's Internet Protection Act ("CIPA"), (iv) New York Education Law Section 2-d, its implementing regulations and the Compliance with Education Law Section 2-d Addendum attached hereto as Exhibit A, (v) any other laws, regulations and statutes, all solely to the extent applicable, and (vi) Discovery's Data Security Policy attached hereto as Exhibit B.



Purchase, Rate, and Downgrade Terms: Public schools in the community or school districts may lock in certain pricing listed in the Services and Pricing section pursuant to the following dates. If a BOCES purchases a product on behalf of a school or district in the period beginning 7/1/2020 and ending 6/30/2021, then that school or district can lock in the 2020-2021 rates for that product until 6/30/2024. If a BOCES purchases a product on behalf of a school or district in the period beginning 7/1/2021 and ending 6/30/2022, then that school or district can lock in the 2021-2022 rates for that product until 6/30/2024. All new school or district subscribers may purchase the DEX Service but will not have the option to purchase the Discovery Education Streaming Service. Current contracted school and district subscribers who have purchased the DEX Service cannot downgrade to Discovery Education Streaming Service. This Discovery Education Streaming Service buying restriction does not affect contract holder's ability to purchase any Discovery services besides the Discovery Education Streaming Service. All pricing beginning 7/1/2022 through 6/30/2024 will be at the sole discretion of Discovery Education.

DocuSigned by:

DISCOVERY EDUCATION, INC.

Signature: 
Name: TRAVIS BATT

Title: COO

Date: November 17, 2020

Exhibit A

Education Law Section 2-d Contract Addendum

The parties to this Contract Addendum are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and Discovery Education, Inc. ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d") and its implementing regulations, and Vendor is a third party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into this Contract Addendum to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of this Contract Addendum, the terms of this Contract Addendum shall apply and be given effect.

Definitions

As used in this Addendum and related documents, the following terms shall have the following meanings:

"Student Data" means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under this Agreement.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

"BOCES" means Monroe #1 Board of Cooperative Educational Services.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student" means any person attending an educational agency who uses Vendor products/services subject to the Master Agreement.

"Eligible Student" means a student eighteen years or older.

"State-protected Data" means Student Data, as applicable to Vendor's product/service.

"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.

"Breach" means the unauthorized access, use, or disclosure of personally identifiable information.

"Commercial or marketing purpose" means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the Student Management Services Agreement (the "Services").

"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement;

(c) not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(d) maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

(e) Discovery Education, Inc., uses encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U.S.);

(f) not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(g) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state and local laws, rules and regulations;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of student data caused by Vendor or its agent or assignee;

(m) ensure that employees, assignees and agents of Contractor who have access to student data, or teacher or principal data will abide by the Discovery Education Student Data Protection Addendum, found on <https://www.discoveryeducation.com/data-protection-addendum/>; and

(n) ensure that any subcontractor that performs Contractor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law.

Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security
(<https://www.monroe.edu/domain/1478>)

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Student Records Policy 6320. (<https://www.monroe.edu/6320>)
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing, to:

Chief Privacy Officer
New York State Education Department
Room 863 EBA
89 Washington Avenue
Albany, New York 12234.

or
Monroe One Data Protection Officer
William Gregory
Monroe #1 BOCES
41 O'Connor Road
Fairport, NY 14450

Supplemental Information About Agreement Between Discovery Education, Inc. and BOCES

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide the Discovery Education licenses and services described in the Agreement to BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) The effective date of this Contract Addendum shall be July 1, 2020 and the Agreement and Addendum shall remain in effect until June 30, 2022, unless sooner terminated in accordance with the terms of the Agreement.

(d) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, Vendor shall securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance with the terms of this Addendum. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(e) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.

(f) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, aligns with NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

DocuSigned by:

7886C13848A0460
Vendor Signature

November 17, 2020

Date

**DISCOVERY EDUCATION, INC. DATA SECURITY POLICY
EXHIBIT B**

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, grade level, and Discovery generated username/password), 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) and who are required to implement administrative, physical, and technical infrastructure and procedural safeguards in accordance with accepted industry standards.

"Authorized Use" 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 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

DocuSign Envelope ID: 968BE934-9BF4-4BC1-B156-D4F5B942ECC4 vices containing the information have appropriate security settings in place (such as encryption, firewall protection, anti-virus software and malware protection).

- g. Any downloaded materials consisting of PII remain in the United States.
- h. Prohibit the unencrypted transmission of information, or any other source of PII, wirelessly or across a public network to any third party.
- i. 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.
- 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.

Security Controls Implementation

DocuSign Envelope ID: 968BE934-9BF4-4BC1-B156-D4F5B942ECC4 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

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 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.



