



BOCES PURCHASE CONTRACT

Region: \_\_\_\_\_ (the "BOCES") Signature: \_\_\_\_\_
Address: \_\_\_\_\_ Name: \_\_\_\_\_
Title: \_\_\_\_\_
Date: \_\_\_\_\_

This BOCES Purchase Contract (the "Contract") is made as of 03/31/2020 by and between the BOCES ("BOCES") and Discovery Education, Inc. ("Discovery").

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.

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)

2020-2021 2021-2022 2022-2024

K-8

K-12 / 9-12

Per student option

(per student per year, available purchase.)

Optional add-on products

DEX Upgrade

Per student option

DEX per student upgrade (per student per year, available only for district-wide purchase)

Discovery Education Experience:

K-8

K-12 / 9-12

Per student option

(per student per year, available only for district-wide purchase)

Discovery Education Coding (requires DE.X service):

K-8

Discovery Education Science:

K-8

Discovery Education Health:

STEM Connect (requires DE.X service):

Professional Learning (On site PD Session, One 6-hour session for up to 25 participants)

DE.X Professional Development Launch Bundle (3 Days)

On-Site Product Training Session

On-Site Professional Learning Sess

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.

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 and comply with the Terms of Use located at https://www.discoveryeducation.com/terms-of-use/.
Market 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.
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.

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.

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 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.

Discovery agrees to comply with the applicable requirements of New York Education Law § 2-d and the Parents Bill of Rights as more fully described in the rider attached hereto as Exhibit B and Exhibit C respectively.



**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.

**DISCOVERY EDUCATION, INC.**

**Signature:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Date:** \_\_\_\_\_



**EXHIBIT A**  
**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, 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 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.
- 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**

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**

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.



**EXHIBIT B**  
**NEW YORK EDUCATION LAW § 2-D COMPLIANCE**

**WHEREAS**, BOCES and Discovery entered into the BOCES Purchase Contract dated 03/31/2020 for purchase of the digital curriculum service(s) known as Discovery Education Streaming, Discovery Education Streaming Plus, Discovery Education Science, Discovery Education Health, and Discovery Education Professional Development (the "Addendum");

**WHEREAS**, BOCES is a New York educational agency subject to all state and federal laws governing education, including but not limited to New York Education Law § 2-d, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

**WHEREAS**, New York State Education Law § 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law § 2-d, educational agencies and certain third party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data and ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data; and

**NOW, THEREFORE**, the Parties agree as follows:

1. Discovery will not release or disclose personally identifiable student information to any party, except to Authorized Disclosees, without prior authorization from the parent or where applicable, the student, unless they have a legitimate interest in the education of the student pursuant to Discovery's Data Security Policy attached hereto as Exhibit B and incorporated by reference herein;
2. Discovery will not sell personally identifiable student information;
3. Discovery agrees to comply with the applicable provisions of the Parents' Bill of Rights attached hereto as Exhibit C;
4. At such time when Discovery's services are no longer required, all personally identifiable student information in Discovery's possession, in whatever form, shall be destroyed by Discovery; and
5. BOCES shall provide written notification of any amendments or modifications to New York Education Law § 2-d or the Parents' Bill of Rights within ten (10) days of such amendment or modification. Upon such amendment or modification, Discovery shall have the option, in its sole discretion, to terminate the Agreement if Vendor cannot meet the obligations set forth in the amendment or modification. Such termination will become effective upon Discovery's ten (10) days written notice to BOCES.



EXHIBIT C

**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.
- (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 for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or 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 the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: [CPO@mail.nysed.gov](mailto:CPO@mail.nysed.gov).

---

Signature

---

Title

---

Date

---

Company