Subscriber Agreement ("Agreement")
made 04/25/2016 between Discovery Education, Inc. ("Discovery") and
SAN LEANDRO UNIFIED SCH DIST, CA ("Subscriber")

1. Subject to the terms and conditions of this agreement, Discovery grants to Subscriber, and the educators, administrators, and students (collectively, "Users") enrolled in the school(s) listed in Exhibit A hereto (the "Community") a limited, non-exclusive, terminable, non-transferable license to access Discovery Education Streaming via the website currently at http://streaming.discoveryeducation.com, or by any other means on which the parties may agree, and to use Discovery Education Streaming as set forth in the Terms of Use located at http://www.discoveryeducation.com/aboutus/terms_of_use.cfm, as Discovery may revise such Terms of Use from time to time (the Discovery Education Subscription Services "Terms of Use").

2. The "Term" shall be 07/01/2016 through and including 06/30/2017.

3. The pricing for this license (the "Fees") shall be as follows (select as applicable):

Discovery Education Streaming PLUS

Quantity	Description	Price/Year	Total
1	Discovery Education Streaming Plus HS License	$3,150.00	$3,150.00
1	Discovery Education Streaming Plus HS License – LE*	$1,550.00	$1,550.00
10	Discovery Education Streaming Plus K-8 License	$2,600.00	$26,000.00
		Total	**$30,700.00**

*LE means enrollment of less than 200 students

4. The Fees are non-cancellable and are due and payable no later than 30 days of receipt of invoice.

5. Subscriber may add schools in the district to this Agreement by written notice to Discovery, setting forth the name and address of the applicable school, the grade level of such schools, the number of students enrolled in each school, and the commencement date of the term for such schools (each, a "School Notice," and which may be submitted in the form of a purchase order). Upon receipt of a School Notice, the schools referenced therein shall be added to this Agreement and their Licenses shall become effective. Fees for additional schools will be prorated, based upon the number months in the term of the License for such additional school. The Fees for the additional schools shall be due and payable no later than thirty (30) days after the commencement date.

6. All other terms and conditions governing this license shall be as set forth in the Terms of Use, and this Agreement, together with the Terms of Use constitute the complete and exclusive terms of the agreement between the parties regarding the subject matter and supersedes all other prior and contemporaneous agreements, negotiations, communications or understandings, oral or written, with respect to the subject matter hereof. There shall be no modifications to this Agreement unless they are in writing, and duly signed by both parties. In no event shall the terms and conditions of a purchase order or any other purchase agreement amend or modify the terms and conditions of this Agreement or the Terms of Use. In the event of a direct conflict between the terms of this Agreement and the terms of the applicable then-current Terms of Use, the terms of this Agreement shall control.

7. While Subscriber acknowledges that no student personal information is required for the use of any of the basic Discovery Education services, in the event Subscriber or its 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, Subscriber represents and warrants that Subscriber has 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, Subscriber consents to Discovery's use of such information in the course of providing the Discovery Education services. Discovery agrees to use any student personal information and data provided to it by Subscriber in compliance with (i) the Children's Online Privacy Protection Act of 1988 ("COPPA"), the Family Educational Rights & Privacy Act of 1974 ("FERPA"), Children's Internet Protection Act ("CIPA") and any other laws, regulations and statutes, all solely to the extent applicable, (ii) Discovery's Data Security Policy attached hereto as Exhibit B, and (iii) Exhibit C.

THE TERMS AND CONDITIONS SET FORTH HEREIN SHALL NOT BE BINDING ON DISCOVERY EDUCATION, INC., OR ANY OF ITS AFFILIATES, UNTIL FULLY EXECUTED BY AN AUTHORIZED SIGNATORY FOR BOTH SUBSCRIBER AND DISCOVERY EDUCATION, INC. (OR ITS APPLICABLE AFFILIATE).

8. Discovery understands that government entities, such as Subscriber, may be required to disclose information pursuant to applicable open records acts. Prior to any such disclosure, Subscriber shall make any claim of privilege that may be applicable to prevent such disclosure and will make reasonable efforts to give Discovery reasonable prior notice and a reasonable opportunity to resist such disclosure. In all other respects, all provisions of this Agreement ("Confidential Information") shall be kept strictly confidential by Subscriber and may not be disclosed without prior written consent, except for any disclosure required by any order of a court or governmental authority with jurisdiction over Subscriber.

9. Subscriber certifies that Subscriber is exempt from all federal, state, and local taxes and will furnish Discovery with copies of all relevant certificates demonstrating such tax-exempt status upon request. In the event Subscriber is not exempt from certain of such taxes, Subscriber agrees to remit payment for such taxes to Discovery.

10. This Agreement contains the entire understanding and supersedes all prior understandings between the parties relating to the subject matter herein. The terms and conditions set forth herein shall not be binding on Discovery, or any of its affiliates, until fully executed by an authorized signatory for both Subscriber and Discovery (or its applicable affiliate). Signatures may be exchanged in counterparts. Signatures transmitted electronically by fax or PDF shall be binding and effective as original ink signatures.

SAN LEANDRO UNIFIED SCH DIST	DISCOVERY EDUCATION, INC.
By: _____ (Signature Required)	By: _____
Title: _____	Title: _____
Printed Name: _____	Printed Name: _____
Date: _____	Date: _____

RETURN THE ATTACHED EXHIBIT A WITH THIS SIGNED AGREEMENT

Billing Entity: _____

Billing Entity Address: _____

_____

Billing Entity Phone Number: _____

Ref. No. O6UJ9C0027GI

THE TERMS AND CONDITIONS SET FORTH HEREIN SHALL NOT BE BINDING ON DISCOVERY EDUCATION, INC., OR ANY OF ITS AFFILIATES, UNTIL FULLY EXECUTED BY AN AUTHORIZED SIGNATORY FOR BOTH SUBSCRIBER AND DISCOVERY EDUCATION, INC. (OR ITS APPLICABLE AFFILIATE).

EXHIBIT A
LICENSED SCHOOLS

DISCOVERY EDUCATION SCHOOL INFORMATION REQUIRED				
SCHOOL NAME	**ADDRESS**	**GRADE LEVELS**	**NO. OF STUDENTS**	**PLUS**
BANCROFT MIDDLE SCHOOL	1150 BANCROFT AVE, SAN LEANDRO, CA 94577	06 - 08	1,045	X
JAMES GARFIELD ELEM SCHOOL	13050 AURORA DR, SAN LEANDRO, CA 94577	K - 05	380	X
JAMES MADISON ELEMENTARY SCH	14751 JUNIPER ST, SAN LEANDRO, CA 94579	K - 05	383	X
JAMES MONROE ELEMENTARY SCHOOL	3750 MONTEREY BLVD, SAN LEANDRO, CA 94578	K - 05	358	X
JOHN MUIR MIDDLE SCHOOL	1444 WILLIAMS ST, SAN LEANDRO, CA 94577	06 - 08	1,089	X
LINCOLN HIGH SCHOOL	2600 TEAGARDEN ST, SAN LEANDRO, CA 94577	09 - 12	51	X
MCKINLEY ELEMENTARY SCHOOL	2150 E 14TH ST, SAN LEANDRO, CA 94577	K - 05	460	X
ROOSEVELT ELEMENTARY SCHOOL	951 DOWLING BLVD, SAN LEANDRO, CA 94577	K - 05	464	X
SAN LEANDRO HIGH SCHOOL	2200 BANCROFT AVE, SAN LEANDRO, CA 94577	09 - 12	2,545	X
THOMAS JEFFERSON ELEM SCHOOL	14300 BANCROFT AVE, SAN LEANDRO, CA 94578	K - 05	516	X
WASHINGTON ELEMENTARY SCHOOL	250 DUTTON AVE, SAN LEANDRO, CA 94577	K - 05	360	X
WOODROW WILSON ELEM SCHOOL	1300 WILLIAMS ST, SAN LEANDRO, CA 94577	K - 05	793	X

Please add additional pages as necessary

RETURN THE ATTACHED EXHIBIT A WITH THIS SIGNED AGREEMENT

THE TERMS AND CONDITIONS SET FORTH HEREIN SHALL NOT BE BINDING ON DISCOVERY EDUCATION, INC., OR ANY OF ITS AFFILIATES, UNTIL FULLY EXECUTED BY AN AUTHORIZED SIGNATORY FOR BOTH SUBSCRIBER AND DISCOVERY EDUCATION, INC. (OR ITS APPLICABLE AFFILIATE).

EXHIBIT B
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 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.

EXHIBIT C
CALIFORNIA ASSEMBLY BILL 1584 COMPLIANCE

WHEREAS, Subscriber and Discovery entered into an Agreement dated 04/25/2016 for the digital curriculum service known as Discovery Education Streaming Plus ("Agreement");

WHEREAS, the Subscriber is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015 between a local education agency and a third-party service provider must include certain terms; and

NOW, THEREFORE, the Parties agree as follows:

1. Any Pupil Records [1] that may be provided to Discovery by Subscriber or its Users shall continue to be the property of and under the control of the Subscriber subject to Discovery's right to use such Pupil Records to provide its services to pupil.

2. The procedures by which pupils may retain possession and control of their own pupil generated content are outlined as follows: A pupil may access and then download its own generated content. It may also delete the content from the Discovery Education Streaming Plus service.

3. The options by which a pupil may transfer pupil-generated content to a personal account are outlined as follows: There are no "personal" user accounts within the Discovery Education Streaming Plus service; however, a pupil may download any pupil-generated content previously uploaded within Discovery Education Streaming Plus and save in the pupil's personal accounts outside of the Discovery Education Streaming Plus service. Please note however that any pupil-generated content that contains any assets from the Discovery Education Streaming Plus service may only be used in connection with the pupil's right to use Discovery Education Streaming Plus.

4. Parents, legal guardians, or eligible pupils may review personally identifiable information in the pupil's records and correct erroneous information by providing written notice to Discovery Education, Inc. at One Discovery Place, Silver Spring, MD 20910.

5. Discovery shall take actions to ensure the security and confidentiality of Pupil Records pursuant to Discovery's Data Security Policy.

6. In the event of an unauthorized disclosure of a Pupil's Records, Discovery shall report to an affected parent, legal guardian, or eligible pupil pursuant to Discovery's Data Security Policy.

7. Discovery shall not use any information in a Pupil Record for any purpose other than those required or specifically permitted by the Agreement, this Exhibit C or Discovery's Data Security Policy.

8. Discovery certifies that a Pupil's Records shall not be retained or available upon expiration of the Agreement pursuant to Discovery Education's Data Security Policy.

[1] Pupil Records as defined by AB 1584 include any information directly related to a pupil that is maintained by the LEA or acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employees. Pupil Records does not include de-identified information (information that cannot be used to identify an individual pupil) used by the third party to (1) improve educational products for adaptive learning purposes and for customized pupil learning; De-identified information, including aggregated de-identified information, (2) demonstrate the effectiveness of the operator's products in the marketing of those products; or for the development and improvement of educational sites, services, or applications.