

**TECHNOLOGY SERVICES AGREEMENT WITH [INSERT PROVIDER NAME]**  
(California Education Code § 49073.1 Compliance)

This Agreement (the "Agreement") is entered into as of 10/5, 2016 ("Effective Date") by and between the Oxnard School District ("District") and [insert Consultant name] ("Consultant"). District and Consultant are sometimes referred to herein as the "Parties" and each a "party".

**WHEREAS**, pursuant to the Technology Service Agreement, Consultant provides [[services for the digital storage, management, and retrieval of pupil records][and][digital educational software]] to the District;

**WHEREAS**, pursuant to Assembly Bill 1584 ("AB 1584"), which was codified under the Education Code as section 49073.1, the California Legislature requires that any agreement entered into, renewed or amended after January 1, 2015 between the District and a third-party Consultant must contain the statements and provisions specified under Education Code section 49073.1(b);

**WHEREAS**, the District is a California school district subject to all state and federal laws governing education, including but not limited to: (i); (ii) the Children's Online Privacy Protection Act, ("COPPA") 15 U.S. 6501; (iii) Federal Educational rights and Privacy Act ("FERPA") 20 U.S.C. section 1232g, 34 C.F.R. Part 99; (iv) SB 1177, Student Online Personal Information Protection Act ("SOPIPA") California Business & Professional Code § 20 U.22584; (v) the Protection of Pupil Rights Act ("PPRA") 20 U.S.C. 1232 (h); (vi) the Health Insurance Portability and Accountability Act (HIPPA) 42 U.S Code 1320(d);

**WHEREAS**, the District owns computerized data that includes personal information and is required, under Civil Code sections 1798.29 and 1798.82 and Government Code section 6252, to disclose any breach of its security systems in an expedited manner;

**WHEREAS**, the District and the Consultant desire that the Technology Services Agreement and the services provided by Consultant comply with AB 1584 and are entering into this Addendum to that effect.

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

1. The Parties intend that this Addendum modifies and amends the existing Technology Services Agreement for the limited purpose of ensuring compliance with the provisions and requirements of AB 1584 as set forth in Education Code section 49073.1. All terms and provisions of the Technology Services Agreement not expressly modified hereby remain in full force and effect.
2. Amendment. The Technology Services Agreement is hereby amended to specifically include the following requirements specified in section 49073.1(b):
  - a. Pupil Records. The Parties acknowledge and agree that, notwithstanding any other provision of the Technology Services Agreement, pupil records (as defined below) are and remain the property of the District and Consultant shall not access, use or dispose of such records except for the purposes contemplated under the Technology Services Agreement or in compliance with the written direction of the District;

As used herein and in the Technology Services Agreement, "pupil records" or "student records" include any information concerning a student that is maintained by the District or acquired from the student or his or her legal guardians through the use of instructional software or applications assigned to the pupil by a teacher or other District employees. Pupil records does not include de-

identified information (information that cannot be used to identify an individual pupil) used by Consultant or other third party to: (1) improve educational products for adaptive learning purposes and for customized pupil learning; (2) demonstrate the effectiveness of a provider's products for marketing purposes; or (3) develop and improvement educational sites, services, or applications.

- b. Pupil-generated content. Notwithstanding the foregoing, pupils may retain possession and control of their own pupil-generated content.

If pupil-generated content is created, Consultant shall provide a specific procedures allowing District students to transfer their pupil-generated content to a personal account. Such procedures shall be attached hereto as an **Attachment**.

- c. Non-Dissemination of Student Information. Consultant shall not use any information in any pupil record for any purpose other than those required or specifically permitted under the Technology Services Agreement;
- d. Correction of Student Records. Consultant shall provide a description of the procedures by which parents or legal guardians or eligible pupils may review and correct, if needed, personally identifiable information;
- e. Confidentiality of Student Records. Consultant shall take actions to ensure the security and confidentiality of pupil records. Such actions shall include but not limited to designating and training responsible individuals on ensuring the security and confidentiality of pupil records. Consultant understands and agrees that enacting these measures will not absolve Consultant of liability in the event of an unauthorized disclosure of pupil records;
- f. Notification. Consultant shall work with District staff to ensure that any parent, legal guardian or eligible pupil affected by an unauthorized disclosure of pupil records is notified;
- g. Disposition of Student Records. Consultant certifies that pupil records will not be retained by, or available to, Consultant or any of its subcontractors or agents upon completion of the services contemplated under the Technology Services Agreement. If any such records are created during the term of that agreement, Consultant shall ensure that they are returned to the District or destroyed, at the District's option and upon the District's written request following notice from Consultant clearly identifying such records. Certification is included as an **Attachment** hereto.
3. Term. This Addendum shall remain in effect while the Technology Services Agreement is in effect and shall expire or terminate, as applicable, concurrently with the Technology Services Agreement.
4. Compliance with FERPA. District agrees to work with Consultant to ensure compliance with FERPA and the Parties will ensure compliance through the following procedures.
5. Attachments. Consultant will provide each of the following applicable procedures, certifications and documentation and the Parties will number the **Attachments** included:

**Attachment 1** – Procedures for a Transfer of Pupil-Generated Content

**Attachment 2** – Protocol for Review and Correction of Student Personally Identifiable Information

**Attachment 3** – Procedures for Ensuring Confidentiality of Pupil Records (Responsible Consultant Staff / Description of Consultant Training)

Attachment 4 - Procedure for Notification of Persons Affected by Unauthorized Disclosure of Pupil Records.

Attachment 5 - Consultant Certification and Procedure to Ensure Non-Retention of Pupil Records.

Attachment 6 - Procedure for Compliance with FERPA.

6. Incorporation of Recitals and Attachments. The Recitals and each certification by Consultant and Attachment identified above are hereby incorporated by this reference to be given full force and effect as if fully set forth herein and in the Technology Services Agreement.
7. The person(s) executing and delivering this Addendum on behalf of Consultant warrant and represent that he/she/they understand the applicable requirements of law, have full power and authority to undertake the actions, commitments and obligations herein undertaken and that by the execution and delivery of this Addendum, Consultant is bound to the terms hereof.

IN WITNESS WHEREOF, the District and the Consultant have executed this Addendum to be effective as of the Effective Date first written hereinabove.

OXNARD SCHOOL DISTRICT

By: R Freeman, Asst. Supt.  
[Name/Title]

Date: 10/7/16

eSpark Learning  
[INSERT CONSULTANT NAME]

By: Kirati Doshi  
[Name/Title] Kirati Doshi, Director of Evolution

Date: 10/5/16

## **Attachment 1**

### **Procedures for a Transfer of Pupil-Generated Content**

At eSpark, we value each student's right to access their generated content. The following are the procedures for requesting transfer of pupil-generated content

1. Submit a request to [privacy@esparklearning.com](mailto:privacy@esparklearning.com) with the following information:
  - a. Student Full Name
  - b. Student Identifier
  - c. Student Grade
  - d. School District Name
  - e. Teacher Name
  - f. Description of the content to transfer
  - g. Email address or secure FTP link where content can be sent
2. Once all of the above information is received, a customer support team member will review the request within 10 business days of receipt
3. Request fulfillment times may vary based on content complexity and size of content. An estimated transfer time will be communicated after reviewing the request - we will do our best to expedite this request and make it a transparent process.

## **Attachment 2**

### **Protocol for Review and Correction of Student Personally Identifiable Information**

Parents may request to review your child's personal information. You may also request to correct, update, or delete your child's personal information from our database. We will be required by law to ensure anyone making such a request is a parent or legal guardian. You may be asked to provide some information, and it may take a few business days to process your request. To make such a request, please contact us using the information provided below.

Please note, that the eSpark program is based upon providing individualized and customized content for its students. The information that we collect is necessary for your child to participate in our program. Should you request your child's complete personal information be deleted and revoke your consent to allow eSpark to collect information about your child, then your child will not be able to participate in the eSpark program.

The following describes the protocol for requesting a review of student personally identifiable information:

1. Submit a request to [privacy@esparklearning.com](mailto:privacy@esparklearning.com) with the following information:
  - a. Your Full Name
  - b. Your relationship to Student
  - c. Student Full Name
  - d. Student Identifier
  - e. Student Grade
  - f. School District Name
  - g. Teacher Name
  - h. Description of personally identifiable information you would like to review
  - i. Email address to which to submit the personally identifiable information
  - j. A contact phone number
2. Once all of the above information is received, a customer support team member will review the request within 10 business days of receipt
3. Request fulfillment times may vary based on request complexity. An estimated time for delivery will be communicated after reviewing the request - we will do our best to expedite this request and make it a transparent process.

If you would like to correct student personally identifiable information, follow the following protocol:

1. Submit a request to [privacy@esparklearning.com](mailto:privacy@esparklearning.com) with the following information:
  - a. Student Full Name
  - b. Student Identifier
  - c. Student Grade
  - d. School District Name
  - e. Teacher Name
  - f. Current information on record that you would like corrected

- g. New information you would like to replace it with
2. Once all of the above information is received, a customer support team member will review the request within 10 business days of receipt
3. Request fulfillment times may vary based on request complexity. An estimated completion time will be communicated after reviewing the request - we will do our best to expedite this request and make it a transparent process.

### **Attachment 3**

#### **Procedures for Ensuring Confidentiality of Pupil Records (Responsible Consultant Staff / Description of Consultant Training)**

The security of student information is extremely important to us. We have implemented technical, administrative and physical security measures which meet or exceed industry standards. We continually review our security procedures in light of the latest threats and industry advances. While we will take all reasonable efforts to protect students' information, no security measures are perfect or impenetrable. Access to information is limited to those employees who require it to perform their job functions through the use of user and password credentials. We use industry-standard Secure Socket Layer (SSL) encryption technology to safeguard student information.

Information collected by eSpark is hosted in and managed and controlled by us from the United States and is not intended to subject us to the laws or jurisdiction of any jurisdiction other than that of the United States. If you are a user located outside the United States, you understand and consent to having any personal information processed in the United States. United States data protection and other relevant laws may not be the same as those in your jurisdiction. This includes the use of cookies and other tracking technologies as described above.

Our full privacy policy can be found here - <https://info.esparklearning.com/privacy>.

**Attachment 4**

**Procedure for Notification of Persons Affected by Unauthorized Disclosure of Pupil Records.**

In the unlikely event of a confirmed data breach of personally identifiable student records, we will immediately notify the impacted key contact at the school or school district of each student. As the information is owned by students, schools, and/or school districts, we will partner with school and district administrators to follow their procedures and protocol to notify impacted individuals and their parents/guardians if appropriate.



**Attachment 5**

**Consultant Certification and Procedure to Ensure Non-Retention of Pupil Records.**

We recognize that the student information shared with us are the property of the student, school and/or district. eSpark certifies that upon written request from a school or district official, student records will not be retained by eSpark upon completion of the services contemplated under the Technology Services Agreement. An authorized school/district official can request to have student records be returned to the school/district or deleted from our systems.

**Attachment 6**

**Procedure for Compliance with FERPA.**

A full description of our data privacy policy demonstrating compliance with FERPA is available here - <https://info.esparklearning.com/privacy>.