TECHNOLOGY SERVICES AGREEMENT WITH AMPLIFY EDUCATION, INC.

(California Education Code § 49073.1 Compliance)

This Agreement (the "Agreement") is entered into as of August 9, 2016 ("Effective Date") by and between the Oxnard School District ("District") and Amplify Education, Inc. ("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 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 ___ – Procedures for a Transfer of Pupil-Generated Content

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

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

Attachment ___ – Procedure for Notification of Persons Affected by Unauthorized Disclosure of Pupil Records.

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

Attachment ___ – 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: Robert Freeman
[Name/Title]

Date: 10/5/16

AMPLIFY EDUCATION, INC.

By: Steven Zavari
[Name/Title] Steven Zavari, Vice President, Science Program

Date: 09/07/2016

ATTACHMENT:

1) **Procedure for Ensuring Confidentiality of Pupil Records (Responsible Consultant Staff / Description of Consultant Training)**

   See attached.

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

   In the event Amplify discovers or is notified of an unauthorized disclosure of pupil records within Amplify's possession or control in violation of applicable federal or state law, Amplify will investigate, take steps to mitigate the potential impact, and provide notice of the breach to applicable agencies, including LEA, as applicable.

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

   Upon termination of the Technology Services Agreement, Amplify will return or destroy personally identifiable information in pupil records.

4) **Procedure for Compliance with FERPA.**

   The parties acknowledge and agree that LEA is subject to federal and state laws relating to the protection of personally identifiable information of students, including FERPA, and that Amplify is obtaining such personally identifiable information as a "school official" under Section 99.31 of FERPA for the purpose of providing the products hereunder. Subject to the terms and conditions of the Technology Services Agreement, Amplify will not take any action to cause LEA to be out of compliance with FERPA or other applicable laws relating to PII

Information Security at Amplify

Last Revised: June 2016

Contents

1. Introduction

The power of data to transform education means having the right data available to the right person at the right time. The challenge for districts and technology providers is to balance this need with the risk that the data will wind up in the wrong hands. This same challenge exists in other industries; for example, in the healthcare world, a drug allergy is a critical part of a patient's health record, but patients don't want this data shared with anyone but their doctor. This information should be visible to any health professional treating the patient but not to anybody else. Education works the same way — a teacher needs the right data about a student at her fingertips when teaching, but this data should not be viewable by anybody the district has not authorized for this purpose.

At Amplify, we build our products with that principle in mind. Student personal information[1] — whether student records provided by schools, or data gathered for schools by using Amplify products — is never used for any purpose other than to improve students'

educational experience. School districts[2] decide who can view this data, and must give permission for sharing this data with any third parties.

In this document we describe some of the key internal organizational controls that Amplify implements to adhere to the above principle and ensure districts retain control of student personal information at all times. While it is not possible to completely secure against all digital threats, we believe that by following the industry best practices described below, we provide appropriate protections for student personal information in our care.

2. Governance

To properly safeguard the data we collect on behalf of school districts, Amplify developed an information security program based on the internationally recognized industry security standard ISO27002. The ISO27002 standard provides a robust framework of security controls from which an organization can build its security protocols based on identified risks, compliance requirements, and business needs. The ISO27002 standard covers access control, change management, training, and other information security domains. By building our information security program around ISO27002, we ensure that we have a comprehensive information protection approach.

Amplify established a Information Security Task Force with primary responsibility for the development, maintenance, and implementation of the Amplify information security program. The Information Security Task Force is responsible for all information risk management activities within the company and is composed of technology, business and legal leaders from the organization

Adherence to the internal Amplify information security policy is an obligation of every Amplify employee. Amplify conducts a series of internal monitoring procedures to verify compliance with internal information security policies, and all Amplify employees undergo annual criminal background checks. In addition, any third-party contractors who come into contact with systems that may contain student personal information are contractually bound to maintain confidentiality of the data.

3. Access Control

Amplify's access control principles dictate that all student personal information we store on behalf of customers is only accessible to district-authorized users and to a limited set of internal Amplify users who may only access the data for purposes authorized by the district. Districts maintain control over their internal users and may grant or revoke access.

In limited circumstances and strictly for the purposes of supporting school districts and maintaining the functionality of systems, certain Amplify users may access Amplify systems with student personal information. All such access to student personal information by Amplify technicians or customer support requires both authentication and authorization to view the information. Amplify logs and monitors such access, which is strictly limited to internal users who ensure the technical functioning of the system or troubleshoot customer issues or otherwise access for purposes authorized by the district. Amplify periodically reviews its internal systems to ensure the necessary security controls are in place to limit access to all systems with personal student information.

4. Securing Data in the Cloud

In the past, organizations ran data centers they physically owned and managed that often consisted of a storage closet with a rack of servers. In recent years, businesses in virtually all industries have started to store even their most sensitive information in highly secure data centers run by other providers. The "cloud" is a general term for using remote servers hosted on the Internet to store, manage, and process data, rather than a local server.

The use of cloud technologies has grown rapidly in recent years, as organizations realize that uptime, physical security, resilience, and support can all be better served through a central facility rather than an onsite data center. In terms of security and privacy, data stored in the cloud is in principle no more or less secure than data stored in a data center — it all depends on the processes and technologies the data owner puts in place to protect the data. Some cloud platforms facilitate better security than local data centers, because they may offer security tools an organization does not have at its disposal within a local data center. But the data owner still needs to make use of those tools for them to be helpful.

Like many school systems themselves, and many other security-conscious organizations, Amplify's current infrastructure is a mixture of dedicated data centers and cloud environments. In this regard, Amplify follows the lead of many organizations that house sensitive information in cloud infrastructures that offer increasingly robust security, resilience, stability, and disaster recovery capabilities.

Amplify currently leverages Amazon Web Services (AWS) as its cloud provider of choice. Within AWS, Amplify leverages Virtual Private Clouds (VPCs) and other AWS services. In addition, we implement our standard security mechanisms to restrict access to the data and services in the cloud. Network segmentation strictly separates production and development systems. Student personal information is encrypted while in transit over public networks.

Data in the cloud always remains under the control of the school district. Like on-premise personal student information, the data stored in the cloud is not visible to anyone except users approved by districts and is only accessed by Amplify personnel to support the technical infrastructure or troubleshoot customer issues.

5. Infrastructure and Environment

Amplify implements internal technical and procedural measures to properly secure the infrastructure and environment of its products.

Restricted Access to Servers

Access to production systems at Amplify is restricted to a limited set of internal Amplify users to support technical infrastructure, troubleshoot customer issues, or other purposes authorized by the district. In addition, Amplify is completing implementation of two-factor authentication methods for access to all production systems. Two-factor authentication involves a combination of something only the user knows and something only the user can access. For example, two-factor authentication for administrative access could involve entering a password as well as entering a one-time passcode sent via text message to the administrator's mobile phone. The use of two-factor authentication reduces the possibility that an unauthorized individual could use a compromised password to access a system.

Network security

Network filtering technologies are used to ensure that production environments with student personal information are properly segmented from the rest of the network. Production environments only have limited external exposure to enable customer access to web interfaces and other services. In addition, Amplify uses firewalls to ensure that development servers have no access to production environments.

Other measures that Amplify takes to secure its operational environment include system monitoring to detect anomalous activity that could indicate potential attacks and breaches.

6. Application Security by Design

Permissions within Amplify applications are designed on the principle that school districts control access to all student data. To facilitate this, Amplify applications are designed so that roles and permissions flow from the district to the individual user. For example, applications that offer schools a way to collect and report on assessment results have a web interface that requires district administrators to authorize individuals to view student personal information.

Building the right roles into applications

Security controls within applications are used to ensure that the desired privacy protections are technically enforced within the system. For example, if a principal is supposed to see only the data related to his or her school, Amplify ensures that, throughout the design and development process, our products restrict principals from seeing records for any students outside his or her school.

To make sure Amplify applications properly enforce permissions and roles, our development teams conduct reviews early in the design process to ensure roles and permissions are an essential component of the design of new applications.

Building security controls into applications

Amplify applications are also developed to minimize security vulnerabilities and ensure industry-standard application security controls are in place. As part of the development process, Amplify has a set of application security standards that all applications handling student personal information are required to follow, including but not limited to:

- Student personal information is secured using industry standard encryption when in transit between end-users and Amplify systems.
- Applications are built with password brute-force attack prevention..
- Sessions expire after a fixed period of time.

We also conduct deeper technical reviews of code for security vulnerabilities that can be exploited to gain unauthorized access to data, common web and mobile vulnerabilities published by industry leaders such as OWASP (Open Web Application Security Project).

7. Information Security Training

At Amplify, we believe that protecting student personal information is the responsibility of all employees. We implemented a comprehensive information security training program that all employees undergo upon initial hire. We also provide information security training for specific departments based on role.

8. Third Party Audits

Amplify periodically engages third-party firms to conduct security assessments of our technical systems to check for security vulnerabilities. The purpose of this testing is to see whether there are any technical vulnerabilities that eluded our normal processes for detecting vulnerabilities in our systems. We select third-party firms on the basis of their experience and reputation in the industry. Third-party testing involves a combination of automated and manual testing to check for vulnerabilities in our systems. These tests are conducted annually, at a minimum.

- 1 "Personal information" means any student information defined as personally identifiable information under FERPA or as personal information under the Children's Online Privacy Protection Act ("COPPA"). This includes the student's name, address, email, social security number and other information that, alone or in combination, would allow a reasonable person in the school community to identify the student with reasonable certainty.
- 2 "School district" means a local educational agency, school network, independent school or other school system.