

**DATA PRIVACY AGREEMENT
BETWEEN THE IRVINE UNIFIED SCHOOL DISTRICT**

AND

Bio-Acoustical Corp.

WHEREAS, the Irvine Unified School District ("District") and Bio-Acoustical Corp. ("Provider") have entered into an agreement ("Agreement") dated 07-01-2021 wherein Provider will perform AERIES electronic upload of vision and hearing testing services (the "Service(s)"); and

WHEREAS, in order to provide the Service described above, Provider may have access to student information, such information generally limited to the data elements listed in Section 13 of this Data Privacy Agreement ("Student Data"), defined as student records under the Family Educational Rights and Privacy Act (FERPA) and California Education Code § 49073.1, among other statutes, which are therefore subject to statutory protection; and

WHEREAS, the parties wish to execute this Data Privacy Agreement ("DPA"), effective as of February 1, 2022, in full compliance with FERPA, California Education Code § 49073.1, and other applicable data privacy laws.

NOW THEREFORE, for good and valuable consideration, the Parties agrees as follows:

PURPOSE

1. District and Provider agree to uphold their responsibilities under all applicable privacy statutes, including FERPA, the Protection of Pupil Rights Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), and AB 1584 (found in Education Code Section 49073.1).

DATA PRIVACY

2. Data Property of District: All Student Data, information, data, and other content provided or transmitted by the District to the Provider, or entered or uploaded under District's user accounts ("Data"), remain the sole property of the District. The District retains exclusive control over Student Data and Data including personal information of District staff, including determining who may access Student Data and how it may be used for legitimate authorized purposes. A parent, legal guardian or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and request the transfer of pupil-generated content to a personal account.

3. Data Access: Provider may access District Data solely to fulfill its obligations under the Agreement.

4. Third Party Access: Provider may not distribute District Data or content to any third party without District's express written consent, unless required by law, and except to subcontractors who have agreed to privacy terms consistent with those in this DPA. Provider will ensure that approved subcontractors adhere to all provisions of this DPA. Deidentified and aggregate information may be used by Provider for the purposes of development and improvement of educational sites, services or applications.

5. Third Party Request: Should a third party contact Provider with a request for District Data, including law enforcement and government entities, Provider shall redirect the third party to request the Data directly from the District unless legally prohibited. Provider shall notify the District in advance of a compelled disclosure to a third party unless legally prohibited.

6. Applicability of COPPA: Provider warrants to District that all data collected directly from children and/or data resulting from tracking children's use of the Service is subject to parental consent and will occur in strict conformity to the requirements of the Children's Online Privacy Protection Act (COPPA). Provider shall obtain such parental consent, unless expressly agreed to otherwise by the parties. Provider may not sell or market Student Data, or use Student Data for sale or marketing purposes, including but not limited to targeted advertising, without express parental consent. However, Provider is not restricted from using anonymous, disaggregate data for marketing purposes, provided that such data cannot be used to identify an individual student.

7. Authorized Use: Provider warrants that the data shared under the Agreement and this DPA shall be used for no purpose other than providing the Service pursuant to the Agreement and/ or otherwise authorized under the statutes referred to in section 1, above.

8. Employees Bound: Provider shall require all employees of Provider and subcontractors who may have access to Student Data to comply with all applicable data privacy laws with respect to the data shared under this DPA.

9. Secure Environment: Provider shall maintain all Data obtained pursuant to this DPA in a secure computer environment and not copy, reproduce or transmit Data obtained pursuant to this DPA except as necessary to provide the Service pursuant to the Agreement. Provider has security measures in place to help protect against loss, misuse and alteration of the Data under Provider's control. When the Service is accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology protects information, using both server authentication and data encryption to help ensure that Data is safe, secure, and available to only authorized users. Provider shall host the Service in a secure server environment that uses a firewall and other advance technology in an effort to prevent interference or access from outside intruders. The Service will require unique account identifiers, usernames and passwords that must be entered each time a client or user signs on.

10. Disposition of Data: Provider shall destroy all Student Data and/or personally identifiable Data obtained under the Agreement and/or this DPA when it is no longer needed to perform the Services, and no later than 60 days following the expiration or termination of the Services provided under the Agreement, unless a reasonable written request for destruction or retention of data is submitted by the District. Nothing in the Agreement or this DPA authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

11. Data Breach Notification: Upon becoming aware of any unlawful or unauthorized access to District Data in possession of Provider and/or stored on equipment used by Provider or in facilities used by Provider, Provider will: notify the District as promptly as possible of the suspected or actual incident; investigate the incident as promptly as possible and provide District with detailed information regarding the incident, including the identity of affected users; provide assistance to the District in notifying affected users by taking commercially reasonable steps to mitigate the effects and to minimize any damage resulting from the incident in accordance with Provider's Data Security Policy. Provider shall obtain permission from District prior to directly notifying users of a breach, unless such notice is required by law.

12. Audit: The District reserves the right to audit and inspect the Provider's compliance with this DPA and applicable laws upon reasonable prior written notice to Provider's principal place of business, during normal business hours, and no more than once per year.

13. Data Requested:

Application Technology Meta Data:

- IP Addresses of users, Use of Cookies etc.

Assessment:

- Standardized Test Scores
- Observation Data

Attendance:

- Student class attendance

Demographics

- Student Permanent I.D. Number
- Date of Birth
- Gender
- Teacher
- Grade Level
- Homeroom

DISTRICT DUTIES

14. District: The District will perform the following duties:

(a) Provide Data: Provide data for the purposes of utilizing the Service in compliance with FERPA.

(b) Precautions: Take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Service and hosted data.

(c) Notification: Notify Provider as promptly as possible of any known or suspected unauthorized access.

AGREEMENT

15. Term The Provider shall be bound by this DPA for the duration of the Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than five (5) years.

16. Priority of Agreements: The Agreement and this DPA shall govern the treatment of Student Data in order to comply with the applicable privacy protections, including those found in FERPA and California Education Code § 49073.1. In the event there is conflict between the terms of this DPA and the Agreement or any other Bid/RFP, license agreement, or contract document(s) in existence, the terms of this DPA shall apply solely with respect to the personally identifiable data provided under the terms of the

Agreement.

17. Successors Bound: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

18. Modification of Agreement: No modification or waiver of any term of this DPA is effective unless mutually agreed to in writing by both parties.

19. Severability. If any term, condition or provision of this DPA is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions will nevertheless continue in full force and effect, and shall not be affected, impaired or invalidated in any way.

20. Governing Law. The terms and conditions of this DPA shall be governed by the laws of the State of California with venue in Orange County, California. This DPA is made in and shall be performed in Orange County, California.

21. Non Waiver. The failure of District or Provider to seek redress for violation of, or to insist upon, the strict performance of any term or condition of this DPA, shall not be deemed a waiver by that party of such term or condition, or prevent a subsequent similar act from again constituting a violation of such term or condition.

IN WITNESS WHEREOF, the parties have executed this Data Privacy Agreement as of the last day noted below.

IRVINE UNIFIED SCHOOL DISTRICT

By: 

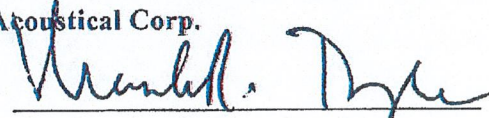
Date: August 18, 2021

Printed Name: John Fogarty

Title/Position: Asst. Supt. Business Services

1USD Board Approved 8/17/2021

Bio-Acoustical Corp.

By: 

Date: 7/9/21

Printed Name: Mark Doyle

Title/Position: President

Note: Electronic signature not permitted.