EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. **Offer of Terms**
Provider offers the same privacy protections found in this DPA between it and **Oak Grove School District** and which is dated 10/26/2020 to any other LEA ("Subscribing LEA") who accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify CETPA in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Provider: Tobii Dynavox LLC

BY: Tara Rudnicki Date: 10/26/2020

Printed Name: Tara Rudnicki Title/Position: President, North American Market

2. **Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Subscribing LEA:

BY: [signature] Date: 6.24.21

Printed Name: E.S. Rossi Title/Position: Assistant Superintendent Educational Services

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW

Name: Alicia Trax

Title: Contract Manager

Email Address: Alicia.Trax@tobiidynavox.com

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Version 2.0 (September 26, 2018)

School District/Local Education Agency:

Oak Grove School District

AND

Provider:

Tobii Dynavox LLC

Date:

10/26/2020

This California Student Data Privacy Agreement ("DPA") is entered into by and between the **Oak Grove School District** (hereinafter referred to as "LEA") and Tobii Dynavox LLC (hereinafter referred to as "Provider") on 10/26/2020 . The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act ("SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A"

hereto: Boardmaker Online Service

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".

4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing

functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing education records under FERPA (4 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill

the Service Agreement.

5. **Disposition of Data**. Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

    a. **Partial Disposal During Term of Service Agreement**. Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3, above.

    b. **Complete Disposal Upon Termination of Service Agreement**. Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition**. Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

b. **Destruction of Data**. Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. **Security Technology**. When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

f. **Security Coordinator**. If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any

identified security and privacy vulnerabilities in a timely manner.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall follow the following process:

    a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

    b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

        i. The name and contact information of the reporting LEA subject to this section.

        ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

        iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

        iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

        v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

    c. At LEA's discretion, the security breach notification may also include any of the following:

        i. Information about what the agency has done to protect individuals whose information has been breached.

        ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

    d. Provider agrees to adhere to all requirements in applicable State and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

    e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law

for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.

4. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

   a. **Designated Representatives**
   The designated representative for the LEA for this Agreement is:

Name: **Najeeb Qasimi**
Title: **The Director of IT**
Contact Information:
6578 Santa Teresa Blvd
San Jose, CA 95119
(408) 227-8300

The designated representative for the Provider for this Agreement is:
Name: Alicia Trax
Title: Contract Manager
Contact Information:
2100 Wharton Street, Suite 400
Pittsburgh, PA 15203
800-344-1778

b. **Notification of Acceptance of General Offer of Terms**. Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.
The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:
Name: Alicia Trax
Title: Contract Manager
Contact Information:
2100 Wharton Street, Suite 400
Pittsburgh, PA 15203
800-344-1778

6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or

enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE IN WHICH THIS AGREEMENT IS EXECUTED, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority**. Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **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.

[Signature Page Follows]

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

Provider: Tobii Dynavox LLC

BY: Tara Rudnicki Date: 10/26/2020

Printed Name: Tara Rudnicki Title/Position: President, North American Market

Local Education Agency:

BY: Najeeb Qasimi Date: 10/26/2020

Printed Name: Najeeb Qasimi Title/Position: Director

EXHIBIT "A"

DESCRIPTION OF SERVICES

Boardmaker Online is a Saas subscription designed:
1) Allow instructors to create or access printed and interactive communication and instructional materials that are fully accessible.
2) Allow instructors to deliver instruction tailored to the special educational needs of each student.
3) Deliver that instructions in a small group setting or directly to the students device.
4) Collect results of student's work and report those to the instructor.

N/A

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	X
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	X
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum program	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	
	Teacher names	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data -Please specify:	
Other	Please list on the next page each additional data element used, stored or collected by your application	

No Student Data Collected at this time _____.

* Provider shall immediately notify LEA if this designation is no longer applicable.

Other: Use this box, if more space is needed.

EXHIBIT "C"

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

Operator: The term "Operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of

instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

SOPIPA: Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and federal laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection,

analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

_____ directs Tobii Dynavox LLC to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

Extent of Disposition Disposition shall be:	____ Partial. The categories of data to be disposed of are as follows: ____ Complete. Disposition extends to all categories of data.
Nature of Disposition Disposition shall be by:	____ Destruction or deletion of data. ____ Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
Timing of Disposition Data shall be disposed of by the following date:	____ As soon as commercially practicable _____By (Insert Date) _____

_____ _____

Authorized Representative of LEA Date

_____ _____

Verification of Disposition of Data Date
by Authorized Representative of Provider

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. **Offer of Terms**
Provider offers the same privacy protections found in this DPA between it and **Oak Grove School District** and which is dated 10/26/2020 to any other LEA ("Subscribing LEA") who accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify CETPA in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Provider: Tobii Dynavox LLC

BY: Tara Rudnicki Date: 10/26/2020

Printed Name: Tara Rudnicki Title/Position: President, North American Market

2. **Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Subscribing LEA:

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW

Name: Alicia Trax

Title: Contract Manager

Email Address: Alicia.Trax@tobiidynavox.com

EXHIBIT "F" DATA SECURITY REQUIREMENTS

Vetted

Boardmaker

United States | Login 0

Assistive Technology
special ed platform

Tobii Dynavox
2100 Wharton St. #400
Pittsburgh, PA 15203

Privacy Policy

General Privacy Policy for the Tobii group – last updated on the 25th of May 2018

Tobii AB (publ) is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using websites, our services or our products (below we use the word "Services" for easier review), you can be assured that it will only be used in accordance with this Pr Policy.

This Privacy Policy outlines how Tobii generally handles your personal data. In connection with some of our Services, we will give you more specific information abc handling of your personal data, and we will, where appropriate, ask for your consent before handling your personal data. At the end of this policy, there is informatic to contact us if you have any questions or if you think anything is unclear.

1. What kind of personal data do we collect?

Depending on which Services you use, we must process different kinds of information from or about you.

Here's how:

Personal data and other information you (and others) give us. We collect the information that you (and others) give us when using our Services. For exampl

When you register to use our Services, we may ask for information such as your name, email address and phone number.

For many of our Services, you will have the opportunity to create a user profile (for example in one of our web-based Services), and add information to yc after registration.

If you buy something from us, we collect information about the transaction. This can include your payment information, purchase activity and delivery and details.

When you communicate with Tobii, you provide us with information such as your email address.

Depending on which Services you use, you have the option of submitting information about your physical features, such as information about your eyes a disabilities concerning your eyes, or other health related data.

If you seek customer support for one of our Services, then it's sometimes necessary for us to access your personal information to be able to help you wit problem (for example if we need to remotely control your device to troubleshoot). In those cases, we will either delete the data once the support matter h resolved (as in the remote control case), or store the data according to applicable retention routines within the Tobii group, if we find that either you or Tc legitimate interest in doing so.

We collect content and information about content that you create using our Services.

Personal data and other information which is automatically collected about you when you use our services. We also collect information automatically wh connected to our Services. Depending on how you access and use our Services, we collect information such as:

Information about how you access our Services, including information about the type of device that you're using, its configuration (such as your operating and graphics processing unit), your browser, and how your device is performing.

Information about the features you interact with on our Services. For example, when you use our devices, we may collect information on how often you us feature, including from third parties.

Information about you and your social media profile if you choose to access our Services with a social media profile. Please note that the information you within the scope of those social media services, is not applicable to this Privacy policy.

Third parties may also collect information about you through the Services, or receive information collected about you through the Services, as described below.

Related companies.
We may share your personal data within the Tobii group in order to develop and improve our products and Services. Such information, however, is anony the best extent possible.

Third party companies.
Some of our Services offers the opportunity to use a social media account as an access method to the Service. If you choose to do so, that social media will receive information that you chose that access method at one of Tobii's Services, and we will receive some types of information from the social media that social media platform processes your information falls outside the scope of this Privacy policy.

2. How do we use your personal data?

We use the information as set out below and to provide our Services to you and our partners. Here's how:

To provide and personalize our Services. We use the information we collect to provide you with our Services. For example, we use this information to:

Communicate with you about our Services;

Provide technical support;

Notify you about updates to our Services; and

Customize your usage based on your activities, including the content, games, apps and other experiences you interact with. This allows us to make our S unique and relevant to you, for example by showing you content that is most relevant to you.

To improve and develop your experience and our Services. We also use the information that we collect to understand, develop and improve our Services. Fo we use the information to:

Seek and analyze input and feedback about our Services;

Identify and address technical issues on our Services;

Conduct and learn from research about the ways in which people use our Services; and

Improve services offered by others, such as third parties that offer games, apps and other content connected to our Services.

To promote our brand and Services. We use the information that we collect to send you promotional messages and content and otherwise market to you on a our Services. We also use this information to measure how users respond to our marketing efforts. If you would like to opt out of receiving marketing emails, thei always do so by follow the instructions implemented in every such promotional message.

To promote safety and security. We use the personal data that we collect to help promote safety and security on and off our Services, such as by investigating activity or breaches of our terms or policies and protecting our or others' rights or property.

3. How is personal data shared?

To provide and support our Services, information that we have about you is shared in certain circumstances. The following can see information about you when you use our Services.

Developers, support and other online content providers on our services. You can interact with Third-party content, games, apps and other experiences thro Services. We may share information about you with these partners so they can provide you with the experiences that you've requested, such as:

Information in your Tobii profile and about how you use our Services. For example, we may provide a third-party games provider with your user id or simil the games provider may deliver a game to you that you've purchased bundled with one of our products

Any other information that you choose to share with the third party through your use of the Services.

Sharing within related companies. Depending on which services you use, we share information with companies that are part of the same group of com Tobii is part of, or that become part of that group, such as Tobii Dynavox, Tobii Pro, and Tobii Tech.

Service providers. We share the information that we collect with vendors, service providers, researchers and other partners, who work at our direction to suppo Services (such as hosting our Services, fulfilling orders, facilitating payments, analyzing the way people use our Services, processing credit card payments, prov customer service or sending electronic communications for us).

Other parties in connection with certain business transactions. In the event that the ownership of Tobii (or any portion of our assets) changes as a result of acquisition or in the event of a bankruptcy, information from or about you or your device may be transferred to another company.

Law enforcement or legal requests. We share information with law enforcement or in response to legal requests in the circumstances outlined in Section 7 be

We also share de-identified or aggregate data with others. "De-identified data" means information where we have removed identifiable data such as your name and that could reasonably be used to identify you. "Aggregate data" is data that has been combined with other data so that it doesn't identify any specific person. For e provide developers with aggregated statistics about the number of people from a particular region that use our Services, so developers can create content tailored in that market.

4. How the Tobii companies work together

Tobii shares infrastructure, systems, and technology with other Tobii companies to provide an innovative, relevant, consistent and safe experience across all Service use.

5. Third parties that provide content, marketing or functionality on our services

Some of the content, marketing and functionality on our Services may be provided by third parties that are not affiliated with us. For example, we work with compar help us provide content within the Service that you purchased.

6. Data retention and deletion

We store data that identifies you until it is no longer necessary to provide our Services, for example when you delete an account with us. This is a case-by-case de that depends on things such as the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, we may re purchase information for accounting and tax purposes even after you have deleted your account.

When you delete an account with us, we delete or anonymize the data you provided us with and the data we collected during your use of the Services. Neither you be able to restore such deleted or anonymized data.

We access, preserve and share information with regulators, law enforcement or others:

In response to a legal request where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction and is c with internationally recognized standards.

When we have a good faith belief that it is necessary to: detect, prevent and address fraud or other illegal activity; to protect Tobii, our Services, you and others, as part of investigations; or to prevent death or imminent bodily harm.

8. How we operate and transfer data as part of our global services

We share information globally, both internally within the Tobii Group and externally with our partners to fully provide the Services you are entitled to receive based o Service you have purchased or subscribed to and/or otherwise are entitled to receive. Information controlled by Tobii will be transferred or transmitted to, or stored processed in the United States, China and/or other countries outside of where you live for the purposes as described in this policy. These data transfers are neces to globally operate and provide our Services to you. We utilize standard contract clauses approved by the European Commission and rely on the European Commi adequacy decisions about certain countries, as applicable, for data transfers from the EU/EEA to the United States and other countries.

9. Changes to this policy

If we make changes to this Privacy Policy, we will provide notice of such changes as appropriate, such as by sending you an email notification to the address that y provided, and/or providing notice through the Services. If we make an administrative change, we may update the "Last Updated" date at the top of this Privacy Poli

The Data Protection Officer for Tobii AB can be contacted at dpo@tobii.com. You also have the right to lodge a complaint with the Swedish lead supervisory autho Datainspektionen, www.datainspektionen.se

10. What is our legal basis for processing data?

The legal ground for processing personal data varies depending on the types of data and the situation. The legal grounds we rely on at Tobii are the following:

If processing is necessary to fulfill our contract with you, i.e. what we are obliged to provide under the agreement between you and us. Our obligations to yc depending on the Service you are using.

For example, we may need to store your name and address to keep track of our warranty obligations to you.

With your consent, which you may withdraw at any time.

For example, when you have given your consent for Tobii to use your eye images and other personal data to develop our algorithms and thus our products.

It should be noted that a withdrawal of a consent shall, and cannot, affect the lawfulness of processing that has already been carried out based on that consent withdrawal.

As necessary to comply with our legal obligations;

For example, Tobii must store some purchase information to comply with tax and accounting regulations. The legal ground for this processing (storing) is therefo necessary for compliance with legal obligations.

Occasionally to protect your vital interests or those of others.

On rare occasions, we may process your data if doing so is necessary to protect your vital interests. For example, in situations where there is an immedia your health we may share information with your caregiver.

As necessary for our (or others) legitimate interests,

Tobii has a legitimate interest in providing an innovative, personalized, safe and profitable service to our existing and future users and partners, unless those inter overridden by your interests or fundamental rights and freedoms that require protection of personal data.

11. How can you exercise the rights provided to you under the GDPR?

Under the General Data Protection Regulation, you have the right to:

Access your data
You have the right to obtain from Tobii a confirmation of whether or not personal data concerning you is being processed, and if that is the case, a right to access it including, but not limited to, the purpose of the processing and the categories of personal data that Tobii has concerning you. By your request, Tobii is required to p with a copy of undergoing processing of your personal data.

Rectify your data
If it comes to your knowledge that certain personal data of yours which is being processed by Tobii is inaccurate, you have the right to obtain a rectification and in s a right to have incomplete data completed.

Port your data
If the legal ground for a processing of personal data is based on either (i) consent or (ii) fulfilment of a contract between you and Tobii, you have a right to receive c

Erase your data
You have the right to obtain from Tobii the erasure of your personal data when, for example, (i) the data no longer is necessary in relation to the purpose for which it collected, (ii) if you withdraw a consent, (iii) if you object to the processing and there are no overriding legitimate grounds for the processing, or if (iv) the personal been unlawfully processed.

Restrict and object to certain processing of your data.
you have the right to restrict Tobii from processing your data when, for example, (i) you contest the accuracy of the personal data, or (ii) if Tobii no longer needs cer for the purposes of the processing.

Find out more about these rights, and how you can exercise them by either contacting Tobii at dpo@tobii.com or obtain information from the appropriate supervisor

12. Contacting us

The data controller responsible for your information is Tobii AB (publ) which you can contact by e-mail at dpo@tobii.com or by post at:

Att: Data Protection Officer
Tobii AB (publ):

Box 743
182 17 Danderyd

Tobii Dynavox LLC and Tobii Dynavox Ltd. are Tobii AB subsidiaries.

FERPA Compliance Statement

In addition to Tobii's general Privacy Policy, the Tobii Dynavox (TD) business has adopted a *Student Data Privacy Policy* that outlines its adherence to FERPA, the L Educational Rights and Privacy Act (20 U.S.C. §1232g, 34 CFR Part 99). TD's *Student Data Privacy Policy* underscores the following commitments:

Records Ownership: TD recognizes that educational records are the property of the educational institution that provides the records to TD.

Access and Requests to Correct Educational Records: TD permits parents and/or eligible students access to their educational records and will work cooper address reasonable requests to correct erroneous information contained within those records.

Limited Usage. TD will only access, collect, store, process, or use educational records as necessary to provide the services set forth in a contract with an educ institution, and for no other purpose. TD will not use the data for any commercial purposes, including for targeted marketing activities.

Confidentiality. TD will treat educational records as confidential. We will limit access within our organization to individuals who need access to such in order to their duties. We will also not re-disclose the educational records to any third-party without the prior written consent of a parent or eligible student.

Data Security. TD protects the security of educational records in its possession consistent with the industry standards referenced below. Additionally, TD woul notification to the educational institution in the event of a breach or suspected breach of student data. Further, TD, will return or destroy all educational records a personally identifiable information in our possession at the conclusion of a contract with an educational institution.

HIPAA Technical Safeguards (42 CFR §164.312) which require, inter alia, computer system access control, unique user IDs, automatic logoff, encryption/decryption, audit controls, etc.

The U.S. Department of Health and Human Services' *Guidance Specifying Technologies and Methodologies that Render Protected Health Information L Unreadable or Indecipherable to Unauthorized* Encryption (g., via encryption and proper destruction) (45 CFR Parts 160 and 164; 74 FR 19006).