

CALIFORNIA STUDENT DATA PRIVACY
AGREEMENT Version 2.0 (September 26, 2018)

School District/Local Education Agency:
Irvine Unified School District

AND

Provider: Bark Technologies, Inc.

Date: May 24, 2021

This California Student Data Privacy Agreement (“DPA”) is entered into by and between the

(hereinafter referred to as “LEA”) and Bark Technologies, Inc. (hereinafter referred to as “Provider”) on May 24, 2021 . 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 services (“Services”), including content monitoring, web filtering, webinars and, as further defined in, and pursuant to the terms of, those Terms of Service located at https://www.bark.us/terms/Bark_School_Monitoring_Terms_of_Service.pdf (“Service Agreement”), which is incorporated herein by this reference; 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 may also be 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, as applicable, 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 (as defined in Exhibit "C") 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:

Products and services designed to promote student safety and health through web monitoring and analysis, and as defined in www.bark.us/schools

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 who have access to Student Data in conjunction with performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a 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 to the extent applicable to Provider's provision of the Service to LEA under the Service Agreement, which may include FERPA, COPPA, PPRA, SOPIPA, AB 1584 and other California privacy statutes.

2. Authorized Use. The Student 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 applicable law. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data 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 such de-identified data is aggregated or generic data, or 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 Student 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 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 delete the 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.

b. Complete Disposal Upon Termination of Service Agreement. Upon written request from LEA after termination of the Service Agreement, Provider shall dispose or delete all Student Data obtained under the Service Agreement.

6. Advertising Prohibition. Provider is prohibited from 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) 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. Provider shall not use Student Data for any marketing or advertising purposes if such use is prohibited by applicable law.

ARTICLE V: DATA PROVISIONS

1. Data Security. The Provider agrees to abide by and maintain commercially reasonable data security measures, consistent with industry standards, 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

industry standards. 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 protocols intended to ensure that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student 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 provide the Services or fulfill the purpose of data requests by LEA.

d. Employee Training. The Provider shall provide periodic security training to those of its employees who are authorized to access Student Data. 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 Student Data 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. If Provider hosts Student Data, Provider shall host such 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 annual) risk assessments and remediate any material identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data in Provider's possession or control is accessed or obtained by an unauthorized individual (a "Security Breach"), Provider shall provide notification to LEA within a reasonable amount of time after Provider becomes aware of the Security Breach, and not exceeding forty-eight (48) hours. Provider shall follow the following process:

a. The security breach notification shall present the information described herein. 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 reasonably 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 reasonably possible to determine at the time the notice is provided.

c. At Provider'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 Security Breach related to the Student Data, including, when required, the required responsibilities and procedures for notification and mitigation of any such Security Breach.

e. Provider further acknowledges and agrees to have a written incident response plan that 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. 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, at LEA's expense unless such unauthorized access was caused by Provider's breach of its obligations under this DPA, 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 caused by Provider's breach of its obligations under this DPA.

g. In the event of a breach originating from LEA's use of the Service, Provider shall use commercially reasonable efforts to cooperate with LEA to the extent necessary to expeditiously secure Student Data, at LEA's sole cost and expense.

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 if Provider fails to cure such breach within thirty (30) days after written notice of same from LEA (to the extent such breach is capable of being cured).

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 applicable 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 and are hereby incorporated into this DPA by reference.

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: Michelle Bennett

Title: Contracts Specialist

Contact Information:

5050 Barranca Pkwy

Irvine, CA 92688

MichelleBennett@iusd.org

The designated representative for the Provider for this Agreement is:

Name: Brian Bason

Title: CEO

Contact Information: 3423 Piedmont Rd
NE, Suite 360, Atlanta, GA 30305

Email: brian@bark.us

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: Brian Bason

Title: CEO

Contact Information:

3423 Piedmont Rd NE, Suite 360, Atlanta,
GA 30305

Email: brian@bark.us

6. Entire Agreement. This DPA and the Service Agreement 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 employees or contractors who may have access to the Student Data and/or any portion thereof from or on behalf of Provider. 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.

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

BY:  Date: April 15, 2021

Printed Name: Brian Bason Title/Position: CEO

Local Education Agency: Irvine Unified School District

BY:  Date: April 19, 2021

Printed Name: John Fogarty Title/Position: Asst Supt Business Services

Note: Electronic signature not permitted

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE]

EXHIBIT "B"
SCHEDULE OF DATA
Category of Data Elements

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:	
Attendance	Student school! (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	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	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
Other indicator information-Please specify:		
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	X
	Other student work data - Please specify:	

Category of Data	Elements	Check if used by your system
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 each additional data element used, stored or collected by your application	X*

*Data contained within content from students' G Suite or Office365 email, cloud document, and cloud storage accounts.

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.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall mean any information that can be used to distinguish or trace an individual’s identity either directly or indirectly through linkages with other information, and may 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 Bark Technologies, Inc.

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 through LEA's use of the Service, 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.

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 gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians through LEA’s use of the Service.

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 an entity that is not Provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

directs 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 which is dated to any other LEA ("Subscribing LEA") who has entered into a separate services agreement with Provider and accepts this General Offer through 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:

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

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: _____

Printed Name: _____

Date: _____

Title/Position: _____

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

Name: _____

Title: _____

Email Address: _____

EXHIBIT "F" DATA SECURITY REQUIREMENTS

N/A

TERMS OF SERVICE

Bark G Suite and Office 365 Offering

Effective date: May 26, 2020

These Terms of Service (“Terms”) govern your use of the Google G Suite and/or Microsoft Office 365 monitoring services of student online activity (the “Service”) made available by Bark Technologies, Inc. (“Bark”, “our” or “we”). *To agree to these Terms, click “I Agree” where indicated in the registration process for the Service.*

Please note your use of the www.bark.us website or related applications (the “Site”) indicates that you agree to be bound by our [Privacy Policy](#) and [Website Terms of Use](#).

1. **Introduction.** The Service is a tool operated by Bark which provides the subscribing school, school district or similar educational entity (“you” or “your”) with a list of, and in some cases email and/or text alerts when potential online dangers (such as cyberbullying) or potential signs of trouble (such as threats, drug abuse, explicit content, depression or similar matters) are identified in email or in designated Google or Microsoft apps involving your registered students (each, a “Covered Account”) using Google Apps or other applications provided through your G Suite services and/or Microsoft Office 365 or other applications provided through your Microsoft service (each service referred to herein individually and collectively as the “Platform”). The Service includes automated review by our proprietary technologies of communications involving the Covered Accounts. The Service currently supports English language interactions only; additional language interactions may become available in the future.
2. **Subscription, Cancellation and Refund Policy.** The Service is offered on a free subscription basis. Subscriptions are month-to-month and automatically renew at the end of each month for the next succeeding month unless you cancel the subscription. To cancel your subscription at any time, please navigate to the “My Account” page on our Site. Bark may terminate this Agreement at any time by providing at least thirty (30) days’ prior written notice to you other than in the event of a material breach of this Agreement by you in which case Bark may immediately terminate this Agreement without notice. Upon cancellation, the Service will terminate and Bark will cease any further review of the Covered Account(s).
3. **Registration.**
 - (a) **General; Administrators; Users.** You must be 18 years of age or older in order to subscribe to the Service. Registration requires you to provide Bark with your name, address, telephone number and email address, and to set up your account as an account administrator (“Administrator”) using a user name and password that you select. You may authorize and set up additional account Administrators and users such as teachers, principals and other representatives participating within your school system who will have access to the Service and will receive alerts provided by the Service as selected by you (each a “User”), provided that all Administrators and Users must be your employees or authorized contractors. You represent and warrant that all information you provide regarding your account, your Administrators and your Users is accurate and up to date and will be kept up to date.
 - (b) **Security/Passwords.** You and your Administrators and Users are responsible for maintaining the confidentiality of your access to the Services. We have no control over use of

user names and passwords and cannot tell whether an unauthorized person is accessing the Services under user names and passwords belonging to your Administrators or Users. You and your Administrators will be responsible for immediately terminating access to the Services for your Administrators and Users who are no longer employed by You or who you no longer wish to have access to the Services. You and your Administrators and Users are solely responsible for any use of the user names and passwords associated with your account by you or any third party. We have no responsibility or liability for any such use. You agree to immediately notify us of any unauthorized use of your account, user name or passwords or any other breach of security that is known or suspected by you.

(c) Students Only. You may register only your students using your Platform to be monitored under your subscription to the Service. You hereby represent and warrant that each student specified for any Covered Account to be monitored by the Service is a student using your Platform.

(d) Covered Accounts. Upon registration, you must identify all Covered Accounts to be monitored by the Service. You must also provide the applications within your Platform to be monitored and the user name and password or other means of authentication of the student for each Covered Account to be connected to the Service. The Covered Account user's log-in information is not stored by Bark but is used to establish our access to the online interactions in the Covered Account. ***For each Covered Account, (i) you represent and warrant that you have the legal authority to access, monitor, review and store online interactions and other communications to and from such Covered Account, including without limitation, all legally required consents from a parent or legal guardian of a Covered Account, and (ii) you expressly authorize Bark to access, monitor, review, and store all online interactions and other communications to and from the Covered Account.*** Administrators on your account may add or remove Covered Accounts through your Google Apps dashboard.

(e) Minimum Age Requirements of Third-Party Platforms. You expressly acknowledge that most third-party platforms are restricted to individuals who are 13 or older, and that, as between you and Bark, compliance with any such age requirement is your sole responsibility.

4. Collection of Student's Information.

(a) Information. During your registration of a Covered Account for the Service, Bark will collect the name and date of birth of the student associated with each Covered Account associated with your account. In connection with providing the Service to you thereafter, Bark will access and monitor communications to and from each Covered Account, which you understand and agree may include communications by or from other children. Bark also collects certain location information regarding the student associated with each Covered Account (including school name and general location).

(b) Consent. You expressly consent to Bark's collection, monitoring and review of any information obtained in connection with a Covered Account, including all communications to and from such Covered Account.

(c) Child Privacy. Questions about Bark's policies or use of information from children under the age of 13 can be directed to Bark Technologies Inc., P.O. Box 1841, Richmond Hill, GA 31324 or at help@bark.us. You may terminate Bark's access, monitoring, collection and/or review of any Covered Account by terminating your subscription by removing Bark from your Google Apps dashboard. The Site and Services do not offer any in application purchases to children under the age of 13.

(d) Disclosure of Information. You acknowledge and agree that the Services may allow you to share the alerts provided to you through the Services which may contain User Data (as defined in the Privacy Policy) of your students (all such shared information referred to herein as your "Shared Information"). We will have no control over your choice to provide access to your Shared Information or the persons to whom you provide access. We will have no liability to you in connection with any access you provide to your Shared Information, including without limitation, liability arising from mistakes that you make in your attempts to provide such access.

5. **Health, Welfare, and Safety Reporting; Contact with Parents.**

(a) We provide alerts to you regarding your student's online activities. If you suspect or determine a threat to the health, welfare, or safety of any individual or entity, you should contact law enforcement or other governmental agencies to make a report. If we identify information that in our sole discretion indicates health, welfare, or safety concerns for an individual or entity, we have the right, but not the obligation, to make reports to law enforcement or other appropriate governmental agencies, and you consent to our authority to do so. The foregoing consent is a condition to your use of the Services.

(b) If you provide us with parent contact information for each Covered Account, we will provide parents of children with Covered Accounts with (i) a welcome message upon commencement of Services, (ii) a weekly message concerning their child's Covered Account activity, and (iii) if directed by you, notification of any reports described in Section 5.a. above.

6. **Alerts.** In some cases Bark will endeavor to send alerts by email to your designated Administrator and User email address(es), or by text to your designated Administrator and User mobile devices (if requested). You are required to maintain updated email or text contact information for your designated Administrators and Users and bear all risks associated with providing Bark with inoperable or incorrect contact information.

7. **Disclaimers. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT:**

(a) **THE SERVICE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, (i) ANY WARRANTY FOR INFORMATION, DATA, DATA PROCESSING SERVICES, OR UNINTERRUPTED ACCESS, (ii) ANY WARRANTY CONCERNING THE AVAILABILITY, ACCURACY, COMPLETENESS, USEFULNESS, OR CONTENT OF INFORMATION, AND (iii) ANY WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE;**

(b) **BARK DOES NOT WARRANT THAT THE SERVICE WILL BE TIMELY, SECURE, UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS WILL BE CORRECTED;**

(c) **BARK MAKES NO WARRANTY THAT THE SERVICE WILL MEET ANY OF YOUR EXPECTATIONS OR REQUIREMENTS; OR THAT USE OF THE SERVICE WILL PROTECT ANY STUDENTS FROM HARM;**

(d) **ANY INFORMATION OBTAINED THROUGH USE OF THE SERVICE IS DELIVERED TO YOU FOR YOUR USE AT YOUR OWN DISCRETION AND RISK, AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE THAT RESULTS FROM BARK'S PROVISION OF OR FAILURE TO PROVIDE ANY SUCH INFORMATION;**

(e) **NO ADVICE, RESULTS OR INFORMATION OR MATERIALS, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU THROUGH THE SERVICE SHALL CREATE ANY WARRANTY NOT EXPRESSLY MADE HEREIN;**

**(f) BARK DOES NOT PROVIDE LEGAL OR MEDICAL ADVICE AS PART OF THE SERVICE;
AND**

**(g) IF YOU ARE DISSATISFIED WITH THE SERVICE, YOUR SOLE REMEDY IS TO
DISCONTINUE USING THE SERVICE.**

8. **Changes to these Terms.** Bark may modify these Terms from time to time. You should check these Terms periodically for modifications. The provisions contained herein supersede all previous notices or statements regarding our Terms with respect to use of the Services. We include the effective date of our Terms at the top of the statement. We encourage you to check our Site frequently to see the current Terms in effect and any changes that may have been made to them. If we make material changes to the Terms, we will post the revised Terms and the revised effective date on this Site, and may notify you of such changes by displaying a notice (or link thereto) on the Site or otherwise. By using the Service following any modifications to these Terms, you agree to be bound by such modifications.

9. **Proprietary Rights.**

(a) Bark (or our licensor) is the owner and/or authorized user of any trademark, registered trademark and/or service mark appearing in connection with the Service, and is the copyright owner or licensee of all content and/or information provided to you through the Service, unless otherwise indicated. Except as otherwise provided herein, use of the Service does not grant you a license to any content, features or materials you may access through the Service and you may not modify, rent, lease, loan, sell, distribute or create derivative works of such Content, features or materials, in whole or in part. Any commercial use of the Service is strictly prohibited, except as allowed herein or otherwise approved by us.

(b) If you make use of the Service other than as provided herein, in doing so you may violate copyright and other laws of the United States, other countries, as well as applicable state laws and may be subject to liability for such unauthorized use. We do not grant any license or other authorization to any user of our trademarks, registered trademarks, service marks, other copyrightable material or any other intellectual property by including them on the Service.

(c) The information on the Service, including, without limitation, all text, graphics, interfaces, and the selection and arrangements is protected by law including copyright law.

(d) Product names, logos, designs, titles, words or phrases may be protected under law as the trademarks, service mark or trade names of Bark or other entities. Such trademarks, service marks and trade names may be registered in the United States and internationally.

(e) The Bark logos and service names are trademarks of Bark (the "Bark Marks"). Without our prior permission, you agree not to display or use Bark Marks in any manner. Nothing on the Site should be construed to grant any license or right to use any Bark Mark without our prior written consent.

(f) **License by You to Use Feedback.** You grant to us and our affiliates a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into the Services any suggestion, enhancement request, recommendation, correction or other feedback provided by you or your Administrators or Users relating to the operation of the Services.

10. **Limitations of Liability.** IN NO EVENT SHALL BARK, ITS AFFILIATES, SERVICE PARTNERS OR ANY OF THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS, OR CONTENT OR SERVICE PROVIDERS BE LIABLE FOR (a) ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES ARISING FROM OR DIRECTLY OR INDIRECTLY RELATED TO THE USE OF, OR THE INABILITY TO USE, THE SERVICE, OR ANY OF THE CONTENT, MATERIALS OR FUNCTIONS RELATED THERETO, INCLUDING, WITHOUT

LIMITATION, LOSS OF REVENUE, OR ANTICIPATED PROFITS, OR LOST BUSINESS, DATA OR SALES, OR COST OF SUBSTITUTE SERVICES, EVEN IF BARK OR ITS REPRESENTATIVE OR SUCH INDIVIDUAL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR (b) AGGREGATE DAMAGES, LOSSES, CLAIMS AND CAUSES OF ACTION (WHETHER IN CONTRACT OR TORT, INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE OR OTHERWISE) ARISING FROM YOUR USE OF THE SERVICE EXCEED, THE AMOUNT OF THE SUBSCRIPTION FEES PAID BY YOU TO BARK. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY SO SOME OF THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. FOR PURPOSES OF THIS AGREEMENT, THE TERM "SERVICE PARTNERS" REFERS COLLECTIVELY TO BARK'S AFFILIATES, RESELLERS, REFERRAL PARTNERS, CONTENT PROVIDERS AND SERVICE PROVIDERS WHO PROVIDE SERVICES TO BARK IN CONNECTION WITH ITS MARKETING, SALE OR PROVISION OF THE SERVICES.

11. **Compliance with Law.** You agree to comply with all applicable laws, rules and regulations in connection with your use of the Service. Without limiting the generality of the foregoing, you agree to comply with all applicable laws regarding the transmission of technical data exported from the United States or the country in which you reside.
12. **Applicable Law/Jurisdiction.** You agree that the laws of the state in which your school or school district is located, excluding its conflicts-of-law rules, shall govern these Terms. Please note that your use of the Service or the Site may be subject to other local, state, national, and international laws.
13. **Class Arbitration.** *Any dispute, controversy or claim arising out of, relating to or in connection with these Terms, including the breach, termination or validity thereof, shall be finally resolved by arbitration. The tribunal shall have the power to rule on any challenge to its own jurisdiction or to the validity or enforceability of any portion of the agreement to arbitrate. The parties agree to arbitrate solely on an individual basis, and that this agreement does not permit class arbitration or any claims brought as a plaintiff or class member in any class or representative arbitration proceeding. The arbitral tribunal may not consolidate more than one person's claims, and may not otherwise preside over any form of a representative or class proceeding.*
14. **Miscellaneous.**
 - (a) The Terms constitute the entire agreement between you and Bark and govern your use of the Service (as the case may be), superseding any prior agreements between you and Bark. You also may be subject to additional terms and conditions that are applicable to certain parts of the Service.
 - (b) You agree that no joint venture, partnership, employment, or agency relationship exists between Bark and you as a result of this Agreement or your use of the Service.
 - (c) Any claim or cause of action you may have with respect to Bark must be commenced within one (1) year after the claim or cause of action arose.
 - (d) The failure of Bark to exercise or enforce any right or provision of the Terms shall not constitute a waiver of such right or provision. If any provision of the Terms is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in the provision, and the other provisions of the Terms remain in full force and effect.
 - (e) You may not assign the Terms or any of your rights or obligations under the Terms without Bark's express written consent.

(f) The Terms inure to the benefit of Bark's successors, assigns and licensees. The section titles in the Terms are for convenience only and have no legal or contractual effect.

(g) Other than the provisions benefiting Bark's Service Partners as set forth in Section 10 hereof, which provisions shall be directly enforceable by such Service Partners, or as otherwise specifically set forth herein, the parties do not confer any rights or remedies upon any third party, including any students, Administrators, Users or any other person or entity other than the parties to this Agreement and their respective successors and permitted assigns.

15. **Notices / Contacting Us.** Bark may notify you via either email or regular mail to the addresses your Administrator provided upon registration of your account or as updated thereafter. Any inquiries you may have concerning these Terms, or to provide any notice to Bark hereunder, should be directed to: Bark Technologies Inc., P.O. Box 18603, Atlanta, GA 31126, with a copy to help@bark.us.

TERMS OF SERVICE

Bark G Suite and Office 365 Offering

Effective date: May 26, 2020

These Terms of Service ("Terms") govern your use of the Google G Suite and/or Microsoft Office 365 monitoring services of student online activity (the "Service") made available by Bark Technologies, Inc. ("Bark", "our" or "we"). *To agree to these Terms, click "I Agree" where indicated in the registration process for the Service.*

Please note your use of the www.bark.us website or related applications (the "Site") indicates that you agree to be bound by our [Privacy Policy](#) and [Website Terms of Use](#).

1. **Introduction.** The Service is a tool operated by Bark which provides the subscribing school, school district or similar educational entity ("you" or "your") with a list of, and in some cases email and/or text alerts when potential online dangers (such as cyberbullying) or potential signs of trouble (such as threats, drug abuse, explicit content, depression or similar matters) are identified in email or in designated Google or Microsoft apps involving your registered students (each, a "Covered Account") using Google Apps or other applications provided through your G Suite services and/or Microsoft Office 365 or other applications provided through your Microsoft service (each service referred to herein individually and collectively as the "Platform"). The Service includes automated review by our proprietary technologies of communications involving the Covered Accounts. The Service currently supports English language interactions only; additional language interactions may become available in the future.
2. **Subscription, Cancellation and Refund Policy.** The Service is offered on a free subscription basis. Subscriptions are month-to-month and automatically renew at the end of each month for the next succeeding month unless you cancel the subscription. To cancel your subscription at any time, please navigate to the "My Account" page on our Site. Bark may terminate this Agreement at any time by providing at least thirty (30) days' prior written notice to you other than in the event of a material breach of this Agreement by you in which case Bark may immediately terminate this Agreement without notice. Upon cancellation, the Service will terminate and Bark will cease any further review of the Covered Account(s).
3. **Registration.**
 - (a) **General; Administrators; Users.** You must be 18 years of age or older in order to subscribe to the Service. Registration requires you to provide Bark with your name, address, telephone number and email address, and to set up your account as an account administrator ("Administrator") using a user name and password that you select. You may authorize and set up additional account Administrators and users such as teachers, principals and other representatives participating within your school system who will have access to the Service and will receive alerts provided by the Service as selected by you (each a "User"), provided that all Administrators and Users must be your employees or authorized contractors. You represent and warrant that all information you provide regarding your account, your Administrators and your Users is accurate and up to date and will be kept up to date.
 - (b) **Security/Passwords.** You and your Administrators and Users are responsible for maintaining the confidentiality of your access to the Services. We have no control over use of

user names and passwords and cannot tell whether an unauthorized person is accessing the Services under user names and passwords belonging to your Administrators or Users. You and your Administrators will be responsible for immediately terminating access to the Services for your Administrators and Users who are no longer employed by You or who you no longer wish to have access to the Services. You and your Administrators and Users are solely responsible for any use of the user names and passwords associated with your account by you or any third party. We have no responsibility or liability for any such use. You agree to immediately notify us of any unauthorized use of your account, user name or passwords or any other breach of security that is known or suspected by you.

(c) Students Only. You may register only your students using your Platform to be monitored under your subscription to the Service. You hereby represent and warrant that each student specified for any Covered Account to be monitored by the Service is a student using your Platform.

(d) Covered Accounts. Upon registration, you must identify all Covered Accounts to be monitored by the Service. You must also provide the applications within your Platform to be monitored and the user name and password or other means of authentication of the student for each Covered Account to be connected to the Service. The Covered Account user's log-in information is not stored by Bark but is used to establish our access to the online interactions in the Covered Account. ***For each Covered Account, (i) you represent and warrant that you have the legal authority to access, monitor, review and store online interactions and other communications to and from such Covered Account, including without limitation, all legally required consents from a parent or legal guardian of a Covered Account, and (ii) you expressly authorize Bark to access, monitor, review, and store all online interactions and other communications to and from the Covered Account.*** Administrators on your account may add or remove Covered Accounts through your Google Apps dashboard.

(e) Minimum Age Requirements of Third-Party Platforms. You expressly acknowledge that most third-party platforms are restricted to individuals who are 13 or older, and that, as between you and Bark, compliance with any such age requirement is your sole responsibility.

4. Collection of Student's Information.

(a) Information. During your registration of a Covered Account for the Service, Bark will collect the name and date of birth of the student associated with each Covered Account associated with your account. In connection with providing the Service to you thereafter, Bark will access and monitor communications to and from each Covered Account, which you understand and agree may include communications by or from other children. Bark also collects certain location information regarding the student associated with each Covered Account (including school name and general location).

(b) Consent. You expressly consent to Bark's collection, monitoring and review of any information obtained in connection with a Covered Account, including all communications to and from such Covered Account.

(c) Child Privacy. Questions about Bark's policies or use of information from children under the age of 13 can be directed to Bark Technologies Inc., P.O. Box 1841, Richmond Hill, GA 31324 or at help@bark.us. You may terminate Bark's access, monitoring, collection and/or review of any Covered Account by terminating your subscription by removing Bark from your Google Apps dashboard. The Site and Services do not offer any in application purchases to children under the age of 13.

(d) Disclosure of Information. You acknowledge and agree that the Services may allow you to share the alerts provided to you through the Services which may contain User Data (as defined in the Privacy Policy) of your students (all such shared information referred to herein as your "Shared Information"). We will have no control over your choice to provide access to your Shared Information or the persons to whom you provide access. We will have no liability to you in connection with any access you provide to your Shared Information, including without limitation, liability arising from mistakes that you make in your attempts to provide such access.

5. **Health, Welfare, and Safety Reporting; Contact with Parents.**

(a) We provide alerts to you regarding your student's online activities. If you suspect or determine a threat to the health, welfare, or safety of any individual or entity, you should contact law enforcement or other governmental agencies to make a report. If we identify information that in our sole discretion indicates health, welfare, or safety concerns for an individual or entity, we have the right, but not the obligation, to make reports to law enforcement or other appropriate governmental agencies, and you consent to our authority to do so. The foregoing consent is a condition to your use of the Services.

(b) If you provide us with parent contact information for each Covered Account, we will provide parents of children with Covered Accounts with (i) a welcome message upon commencement of Services, (ii) a weekly message concerning their child's Covered Account activity, and (iii) if directed by you, notification of any reports described in Section 5.a. above.

6. **Alerts.** In some cases Bark will endeavor to send alerts by email to your designated Administrator and User email address(es), or by text to your designated Administrator and User mobile devices (if requested). You are required to maintain updated email or text contact information for your designated Administrators and Users and bear all risks associated with providing Bark with inoperable or incorrect contact information.

7. **Disclaimers. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT:**

(a) **THE SERVICE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, (i) ANY WARRANTY FOR INFORMATION, DATA, DATA PROCESSING SERVICES, OR UNINTERRUPTED ACCESS, (ii) ANY WARRANTY CONCERNING THE AVAILABILITY, ACCURACY, COMPLETENESS, USEFULNESS, OR CONTENT OF INFORMATION, AND (iii) ANY WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE;**

(b) **BARK DOES NOT WARRANT THAT THE SERVICE WILL BE TIMELY, SECURE, UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS WILL BE CORRECTED;**

(c) **BARK MAKES NO WARRANTY THAT THE SERVICE WILL MEET ANY OF YOUR EXPECTATIONS OR REQUIREMENTS; OR THAT USE OF THE SERVICE WILL PROTECT ANY STUDENTS FROM HARM;**

(d) **ANY INFORMATION OBTAINED THROUGH USE OF THE SERVICE IS DELIVERED TO YOU FOR YOUR USE AT YOUR OWN DISCRETION AND RISK, AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE THAT RESULTS FROM BARK'S PROVISION OF OR FAILURE TO PROVIDE ANY SUCH INFORMATION;**

(e) **NO ADVICE, RESULTS OR INFORMATION OR MATERIALS, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU THROUGH THE SERVICE SHALL CREATE ANY WARRANTY NOT EXPRESSLY MADE HEREIN;**

**(f) BARK DOES NOT PROVIDE LEGAL OR MEDICAL ADVICE AS PART OF THE SERVICE;
AND**

**(g) IF YOU ARE DISSATISFIED WITH THE SERVICE, YOUR SOLE REMEDY IS TO
DISCONTINUE USING THE SERVICE.**

8. **Changes to these Terms.** Bark may modify these Terms from time to time. You should check these Terms periodically for modifications. The provisions contained herein supersede all previous notices or statements regarding our Terms with respect to use of the Services. We include the effective date of our Terms at the top of the statement. We encourage you to check our Site frequently to see the current Terms in effect and any changes that may have been made to them. If we make material changes to the Terms, we will post the revised Terms and the revised effective date on this Site, and may notify you of such changes by displaying a notice (or link thereto) on the Site or otherwise. By using the Service following any modifications to these Terms, you agree to be bound by such modifications.
9. **Proprietary Rights.**
- (a) Bark (or our licensor) is the owner and/or authorized user of any trademark, registered trademark and/or service mark appearing in connection with the Service, and is the copyright owner or licensee of all content and/or information provided to you through the Service, unless otherwise indicated. Except as otherwise provided herein, use of the Service does not grant you a license to any content, features or materials you may access through the Service and you may not modify, rent, lease, loan, sell, distribute or create derivative works of such Content, features or materials, in whole or in part. Any commercial use of the Service is strictly prohibited, except as allowed herein or otherwise approved by us.
- (b) If you make use of the Service other than as provided herein, in doing so you may violate copyright and other laws of the United States, other countries, as well as applicable state laws and may be subject to liability for such unauthorized use. We do not grant any license or other authorization to any user of our trademarks, registered trademarks, service marks, other copyrightable material or any other intellectual property by including them on the Service.
- (c) The information on the Service, including, without limitation, all text, graphics, interfaces, and the selection and arrangements is protected by law including copyright law.
- (d) Product names, logos, designs, titles, words or phrases may be protected under law as the trademarks, service mark or trade names of Bark or other entities. Such trademarks, service marks and trade names may be registered in the United States and internationally.
- (e) The Bark logos and service names are trademarks of Bark (the "Bark Marks"). Without our prior permission, you agree not to display or use Bark Marks in any manner. Nothing on the Site should be construed to grant any license or right to use any Bark Mark without our prior written consent.
- (f) License by You to Use Feedback. You grant to us and our affiliates a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into the Services any suggestion, enhancement request, recommendation, correction or other feedback provided by you or your Administrators or Users relating to the operation of the Services.
10. **Limitations of Liability.** IN NO EVENT SHALL BARK, ITS AFFILIATES, SERVICE PARTNERS OR ANY OF THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS, OR CONTENT OR SERVICE PROVIDERS BE LIABLE FOR (a) ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES ARISING FROM OR DIRECTLY OR INDIRECTLY RELATED TO THE USE OF, OR THE INABILITY TO USE, THE SERVICE, OR ANY OF THE CONTENT, MATERIALS OR FUNCTIONS RELATED THERETO, INCLUDING, WITHOUT

LIMITATION, LOSS OF REVENUE, OR ANTICIPATED PROFITS, OR LOST BUSINESS, DATA OR SALES, OR COST OF SUBSTITUTE SERVICES, EVEN IF BARK OR ITS REPRESENTATIVE OR SUCH INDIVIDUAL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR (b) AGGREGATE DAMAGES, LOSSES, CLAIMS AND CAUSES OF ACTION (WHETHER IN CONTRACT OR TORT, INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE OR OTHERWISE) ARISING FROM YOUR USE OF THE SERVICE EXCEED, THE AMOUNT OF THE SUBSCRIPTION FEES PAID BY YOU TO BARK. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY SO SOME OF THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. FOR PURPOSES OF THIS AGREEMENT, THE TERM "SERVICE PARTNERS" REFERS COLLECTIVELY TO BARK'S AFFILIATES, RESELLERS, REFERRAL PARTNERS, CONTENT PROVIDERS AND SERVICE PROVIDERS WHO PROVIDE SERVICES TO BARK IN CONNECTION WITH ITS MARKETING, SALE OR PROVISION OF THE SERVICES.

11. **Compliance with Law.** You agree to comply with all applicable laws, rules and regulations in connection with your use of the Service. Without limiting the generality of the foregoing, you agree to comply with all applicable laws regarding the transmission of technical data exported from the United States or the country in which you reside.
12. **Applicable Law/Jurisdiction.** You agree that the laws of the state in which your school or school district is located, excluding its conflicts-of-law rules, shall govern these Terms. Please note that your use of the Service or the Site may be subject to other local, state, national, and international laws.
13. ***Class Arbitration. Any dispute, controversy or claim arising out of, relating to or in connection with these Terms, including the breach, termination or validity thereof, shall be finally resolved by arbitration. The tribunal shall have the power to rule on any challenge to its own jurisdiction or to the validity or enforceability of any portion of the agreement to arbitrate. The parties agree to arbitrate solely on an individual basis, and that this agreement does not permit class arbitration or any claims brought as a plaintiff or class member in any class or representative arbitration proceeding. The arbitral tribunal may not consolidate more than one person's claims, and may not otherwise preside over any form of a representative or class proceeding.***
14. **Miscellaneous.**
 - (a) The Terms constitute the entire agreement between you and Bark and govern your use of the Service (as the case may be), superseding any prior agreements between you and Bark. You also may be subject to additional terms and conditions that are applicable to certain parts of the Service.
 - (b) You agree that no joint venture, partnership, employment, or agency relationship exists between Bark and you as a result of this Agreement or your use of the Service.
 - (c) Any claim or cause of action you may have with respect to Bark must be commenced within one (1) year after the claim or cause of action arose.
 - (d) The failure of Bark to exercise or enforce any right or provision of the Terms shall not constitute a waiver of such right or provision. If any provision of the Terms is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in the provision, and the other provisions of the Terms remain in full force and effect.
 - (e) You may not assign the Terms or any of your rights or obligations under the Terms without Bark's express written consent.

(f) The Terms inure to the benefit of Bark's successors, assigns and licensees. The section titles in the Terms are for convenience only and have no legal or contractual effect.

(g) Other than the provisions benefiting Bark's Service Partners as set forth in Section 10 hereof, which provisions shall be directly enforceable by such Service Partners, or as otherwise specifically set forth herein, the parties do not confer any rights or remedies upon any third party, including any students, Administrators, Users or any other person or entity other than the parties to this Agreement and their respective successors and permitted assigns.

15. **Notices / Contacting Us.** Bark may notify you via either email or regular mail to the addresses your Administrator provided upon registration of your account or as updated thereafter. Any inquiries you may have concerning these Terms, or to provide any notice to Bark hereunder, should be directed to: Bark Technologies Inc., P.O. Box 18603, Atlanta, GA 31126, with a copy to help@bark.us.

CALIFORNIA STUDENT DATA PRIVACY

AGREEMENT Version 2.0 (September 26, 2018)

School District/Local Education Agency:

AND

Provider: Bark Technologies, Inc.

Date:

This California Student Data Privacy Agreement (“DPA”) is entered into by and between the

(hereinafter referred to as “LEA”) and Bark Technologies, Inc. (hereinafter referred to as “Provider”) on



_____ . 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 services (“Services”), including content monitoring, web filtering, webinars and, as further defined in, and pursuant to the terms of, those Terms of Service located at https://www.bark.us/terms/Bark_School_Monitoring_Terms_of_Service.pdf (“Service Agreement”), which is incorporated herein by this reference; 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 may also be 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, as applicable, 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 (as defined in Exhibit "C") 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

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:

Products and services designed to promote student safety and health through web monitoring and analysis, and as defined in www.bark.us/schools

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.

3

5. Subprocessors. Provider shall enter into written agreements with all Subprocessors who have access to Student Data in conjunction with performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a 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 to the extent applicable to Provider's provision of the Service to LEA under the Service Agreement, which may include FERPA, COPPA, PPRA, SOPIPA, AB 1584 and other California privacy statutes.

2. Authorized Use. The Student 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 applicable law. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data 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 such de-identified data is aggregated or generic data, or 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 Student 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 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 delete the 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.

b. Complete Disposal Upon Termination of Service Agreement. Upon written request from LEA after termination of the Service Agreement, Provider shall dispose or delete all Student Data obtained under the Service Agreement.

6. Advertising Prohibition. Provider is prohibited from 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) 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. Provider shall not use Student Data for any marketing or advertising purposes if such use is prohibited by applicable law.

ARTICLE V: DATA PROVISIONS

1. Data Security. The Provider agrees to abide by and maintain commercially reasonable data security measures, consistent with industry standards, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of

5

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

industry standards. 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 protocols intended to ensure that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student 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 provide the Services or fulfill the purpose of data requests by LEA.

d. Employee Training. The Provider shall provide periodic security training to those of its employees who are authorized to access Student Data. 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 Student Data 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. If Provider hosts Student Data, Provider shall host such 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 annual) risk assessments and remediate any material identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data in Provider's possession or control is accessed or obtained by an unauthorized individual (a "Security Breach"), Provider shall provide notification to LEA within a reasonable amount of time after Provider becomes aware of the Security Breach, and not exceeding forty-eight (48) hours. Provider shall follow the following process:

a. The security breach notification shall present the information described herein. 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 reasonably 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 reasonably possible to determine at the time the notice is provided.

c. At Provider'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 Security Breach related to the Student Data, including, when required, the required responsibilities and procedures for notification and mitigation of any such Security Breach.

e. Provider further acknowledges and agrees to have a written incident response plan that 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. 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, at LEA's expense unless such unauthorized access was caused by Provider's breach of its obligations under this DPA, 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 caused by Provider's breach of its obligations under this DPA.

g. In the event of a breach originating from LEA's use of the Service, Provider shall use commercially reasonable efforts to cooperate with LEA to the extent necessary to expeditiously secure Student Data, at LEA's sole cost and expense.

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 if Provider fails to cure such breach within thirty (30) days after written notice of same from LEA (to the extent such breach is capable of being cured).

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 applicable 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 and are hereby incorporated into this DPA by reference.

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

8

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: _____ Title:

Contact Information:

The designated representative for the Provider for this Agreement is:

Name: Brian Bason

Title: CEO

Contact Information: 3423 Piedmont Rd
NE, Suite 400, Atlanta, GA 30305

Email: brian@bark.us

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: Brian Bason

Title: CEO

Contact Information:

3423 Piedmont Rd NE, Suite 400, Atlanta,
GA 30305

Email: brian@bark.us

6. Entire Agreement. This DPA and the Service Agreement 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

9

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 employees or contractors who may have access to the Student Data and/or any portion thereof from or on behalf of Provider. 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:

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

Local Education Agency:

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

Note: Electronic signature not permitted.

11

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE]

EXHIBIT “B”
SCHEDULE OF DATA
Category of
Data Elements

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:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	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	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	X

Category of Data	Elements	Check if used by your system
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	

Category of Data	Elements	Check if used by your system
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	X
	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 each additional data element used, stored or collected by your application	X*

*Data contained within content from students' G Suite or Office365 email, cloud document, and cloud storage accounts.

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.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall mean any information that can be used to distinguish or trace an individual’s identity either directly or indirectly through linkages with other information, and may 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 Bark Technologies, Inc.

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 through LEA's use of the Service, 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.

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 gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians through LEA’s use of the Service.

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 an entity that is not Provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

directs 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:

by:

____ Destruction or deletion of data.

Extent of Disposition

____ 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.

Disposition shall be:

____ Partial. The categories of data to be disposed of are as follows:

Timing of Disposition

____ Complete. Data shall be disposed of by all categories of data. the following date:

____ As soon as commercially practicable

Nature of Disposition

____ By (Insert Date)

Disposition shall be

_____ 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 and which is dated (‘‘Subscribing LEA’’) who has entered into a separate services agreement with Provider and accepts this General Offer signature below. This General Offer shall extend only to privacy protections and Provider’s signature shall not neces Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this D and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unio LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy s material change in the services and products subject listed in the Originating Service Agreement; or three (3) years a Provider’s signature to this Form. Provider shall notify CETPA in the event of any withdrawal so that this informatio transmitted to the Alliance’s users. Provider:

BY: _____

Printed Name: _____

2. Subscribing LEA

Date: _____

Title/Position: _____

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

Subscribing LEA:

Date: _____

BY: _____

Title/Position: _____

Printed Name: _____

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

Name: _____

Title: _____

Email Address: _____

20

EXHIBIT "F" DATA SECURITY REQUIREMENTS

N/A

00618-00001/4274378.1