

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

School District/Local Education Agency:

Duarte Unified School District

AND

Provider:

Blackboard Inc.

Date: September 24, 2020

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Duarte Unified School District

(hereinafter referred to as "LEA") and Blackboard Inc. (hereinafter referred to as "Provider" or "Blackboard"). The Parties agree to on _____, 2020 the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with one, all, or a combination of the following: Blackboard Mass Notification/Blackboard Connect, Blackboard Web Community Manager, Blackboard Social Media Manager, and Blackboard Mobile Application, ("Service(s)") pursuant to the agreement between Blackboard and LEA effectively dated July 1, 2013 and April 1, 2017, respectively ("Services") ("Service Agreement"); and

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

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

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

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

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

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

ARTICLE I: PURPOSE AND SCOPE

1. Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official (as

defined in Exhibit C) 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 with respect to Contractor's specific provisions of Services to the LEA.

2. Nature of Services Provided. The Provider has agreed to provide one or more of the digital educational products and services as outlined in Exhibit "A" hereto and as indicated in the Service Agreement:
3. Student Data to Be Provided. The Parties shall indicate the necessary Student Data that may include the categories of Student Data to be provided in the Schedule of Data, attached hereto as Exhibit "B".
4. DPA Definitions. The definitions of the terms used in this DPA are 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 provided by LEA to Provider pursuant to 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, all procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. In the event LEA cannot review and amend the Student Data on its own, 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 guardian 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. Notwithstanding the foregoing, the Services contemplated herein will not require any Pupil Generated Content, and as such, Provider shall not be required to transfer Pupil Generated Content to a separate student account.

4. Third Party Request. Should a Third Party, including law enforcement and government entities, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the Student Data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited from providing such notice.

5. Subprocessors. Provider shall enter into written agreements with all Subprocessors who has access to Student Data and how are performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner materially consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. Privacy Compliance. LEA shall provide Student Data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRa, SOPIPA, AB 1584 and all other California privacy statutes, as applicable.
2. Annual Notification of Rights. If the LEA has a policy of disclosing education records under FERPA (4 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.
3. Reasonable Precautions. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted data.
4. Unauthorized Access Notification. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. Privacy Compliance. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRa, SOPIPA, AB 1584 and all other California privacy statutes as they relate the collection, use, storage, or sharing of Student Data.
2. Authorized Use. The Student Data shared pursuant to the Service Agreement, including persistent unique Identifiers, that reasonably lead to the identity of an individual, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the Service Agreement and the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, unless permitted under the Service Agreement, 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 materially similar provisions to those provisions outlined in this DPA with respect to the Student Data shared under the Service Agreement.
4. No Disclosure. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any

other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b).

Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to

attempt re-identification. 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 or as otherwise permitted herein or in 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 transfer, 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 PII 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. Upon LEA's request, Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will promptly provide the LEA with any specified portion of the Student Data in a commercially reasonable time, unless a shorter time is required by California law and then in such shorter time period.

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

b. Complete Disposal Upon Termination of Service Agreement. Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above.

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

ARTICLE V; DATA PROVISIONS

- 1. Data Security.** The Provider agrees to abide by and maintain adequate data security measures, ~~Consistent~~ with industry standards, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of

Provider are set forth below. 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 industry standards. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Subject to applicable law, all employees hired after 1/1/2011 with access to Student Data shall pass criminal background checks.
- 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. Upon request, Provider shall transfer said data, as available, 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 aligned with industry standard practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student Data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Service Agreement, except as necessary to fulfill the provisioning of the Services or the purpose of Student Data requests by LEA.
- d. Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the systems that store Student Data. Further, upon request by the LEA, Provider shall provide LEA with contact information who LEA may contact if there are any security concerns or questions.
- e. Security Technology.** When the Service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect Student Data from unauthorized access. The security measures shall include server authentication and data encryption. Provider shall host Student Data pursuant to the Service Agreement in an environment the employs boundary protection mechanisms (e.g. firewalls) that are periodically updated according to commercially reasonable industry standards.
- f; Security Coordinator.** If different from the designated representative identified in Article VII, section 5 and upon request by LEA, 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 materially consistent with the terms of this Article V. Provider will remain responsible for

Subprocessors compliance with the obligations of this DPA and for any acts or omissions of the Subprocessors that cause Provider to breach any of the Provider's obligations under this DPA to the same extent Provider would be liable if performing the Services itself.

- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Provider has knowledge or reasonable belief that Student Data has been accessed or obtained by an unauthorized individual ("Data Breach"), Provider shall provide notification to LEA within ten (10) days of the Data Breach. Provider shall follow the following process:

- a.** The Data Breach notification shall be written in plain language and shall present the information described herein, as available. Additional information may be provided as a supplement to the notice.
- b.** The Data Breach notification described above in section 2(a) shall include the following information as available:
 - i.** The name and contact information of the reporting LEA subject to this section.
 - ii.** A list of the types of PII that were or are reasonably believed to have been the subject of a Data Breach.
 - iii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the Data Breach, (2) the estimated date of the Data Breach, or (3) the date range within which the Data 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 Data Breach, if that information is possible to determine at the time the notice is provided.
- c.** At LEA's request, the Data Breach notification to the LEA will also include the following as it becomes available:
 - i.** Information about what the agency has done to protect individuals whose information has been breached.
 - ii.** To the extent required under California law, 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 applicable requirements in California Data Breach law and in federal law with respect to a Data Breach related to the PII, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Data Breach.

- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, Provider shall reasonably assist the LEA with their legally required notifications to the affected parent, legal guardian or eligible pupil of the Data Breach, which shall include the information listed in subsections (b) and (c), above. The LEA remains ultimately responsible for the timing and content of such legally required notifications. If, due to a Data Breach which is caused by Blackboard or our agents' acts or omissions, any third-party notification is required under California law, we shall be responsible for the cost of such notifications.
- g. In the event of a Data Breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data and any third party notifications, if any, shall be at the LEA's 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 a Subscribing LEA (as defined in Exhibit C) who signs the acceptance in said Exhibit solely for the purchase or renewal of the Services outlined in Exhibit A and under a mutual Master Service Agreement (i.e. Services Agreement) which references and incorporates this DPA. 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.** **E i t h e r** party may terminate this DPA and the Service Agreement if the other party materially breaches any terms of this DPA and fails to cure such material breach within thirty (30) days written notice such material breach.
3. **Effect of Termination Survival.** If this DPA is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article V, section 1(b) 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 terms of this DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph p.rin, all other provisions of the Service Agreement shall remain in effect.

5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in in writing and given by personal delivery, or e-mail transmission (if contact information is

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: Eric Ramos

Title: Chief Technology Officer

Contact Information:

1620 Huntington Dr

Duarte, CA 91010

(626) 599 - 5059

The designated representative for the Provider for this Agreement is:

Name: Attn: General Counsel

Address 11720 Plaza America Drive 10th floor, Reston, VA 20190

Email privacy@blackboard.com

6. **Entire Agreement.** 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.
10. **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: **Blackboard Inc.**

BY:  Date: 9/24/20

Printed Name: Bill Jones Title/Position: Deputy General Counsel

Local Education Agency: Duarte Unified School District

BY:  Date: 6-29-20

Printed Name: **Eric Ramos** Title/Position: Chief Technology Officer

Note: Electronic signature not permitted.

EXIHIBIT "A"

DESCRIPTION OF SERVICES

The following is a list of Services that may be purchased or renewed pursuant to this DPA. The actual Services purchased by an LEA shall be addressed in the Agreement between LEA and Provider.

- Blackboard Web Community Manager
- Blackboard Mobile Communications
App Blackboard Connect (select markets only)
- Blackboard Mass Notification
- Blackboard Social Media Manager
- Blackboard Ally

EXHIBIT "B"
SCHEDULE OF DATA

**Please note, the Schedule of Data contains categories of data that may be provided to use the Service(s).
What is actually provided is at the discretion of the LEA.*

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify: e.g., information captured in logs	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify: e.g., test scores and number of attempts	X
Attendance	Student school (daily) attendance data	X
	Student class attendance data	X
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	X
	Place of Birth	X
	Gender	X
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	X
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	X
	Specific curriculum programs	X
	Year of graduation	X
	Other enrollment information-Please specify: e.g., Other student data	X

Category of Data	Elements	Check if used by your system
	elements can be made available in the WCM Dashboard (which uses BB Comms Data): Class Schedule, Attendance information, etc.	
Parent/Guardian Contact Information	Address	X
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language learner information	X
	Low income status	X
	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	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Vendor/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X

Category of Data	Elements	Check if used by your system
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures etc.	X
	Other student work data - Please specify: Student generated content is unlikely but possible in WCM.	X
Transcript	Student course grades	X
	Student course data	X
	Student course grades/performance scores	X
	Other transcript data -Please specify:	
Transportation	Student bus assignment	X
	Student pick up and/or drop off location	X
	Student bus card ID number	X
	Other transportation data - Please specify: Other transportation related information that the client may elect to process/store.	X
Other	Please list each additional data element used, stored or collected by your application: Other student data elements can be made available in the WCM Dashboard (which uses BB Comms Data): Assignments, Grades, Lunch Balances, etc.	X

EXHIBIT "C"

DEFINITIONS

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

De-Identified Information (DII): The terms “De-Identified Information” or “DII” shall mean information that once included Personally Identifiable Information ("PII") but such PII has been removed or obscured by the Provider 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 may constitute Student Data.

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

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

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to any individual and shall include, but are not limited to, Student Data, metadata, 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 may include the categories of information listed in the definition of Student Data.

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

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

Pupil Records: the term “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 Educational Records may be the same as Pupil Records. Pupil Records may constitute Student Data.

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: the term “Student Data” means any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that includes PII 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 DPA, 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.

SDPQ (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: A “Subscribing LEA” means a K12 school district in the State of California purchasing or renewing one or more of the Services outlined herein that was not party to the Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising : Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student personally identifiable information, PII included in the student records or PII included in student generated content. o

Third Party: The term "Third Party" means an entity that is not the Provider or LEA. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF PII

Duarte Unified School District

directs **Blackboard, Inc.**

to

Name or District or LEA] directs Blackboard to dispose of data obtained by Blackboard pursuant to the terms of the Service Agreement between LEA and Blackboard. The terms of the Disposition are set forth below:

<p><u>Extent of Disposition</u></p> <p>Disposition shall be:</p>	<p>____ Partial. The categories of data to be disposed of are as follows:</p> <p>____ Complete. Disposition extends to all categories of data.</p>
<p><u>Nature of Disposition</u></p> <p>Disposition shall be by:</p>	<p>Destruction or deletion of data.</p> <p>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.</p>
<p><u>Timing of Disposition</u></p> <p>Data shall be disposed of by the following date:</p>	<p>____ As soon as commercially practicable</p> <p>____ By (Insert Date) _____</p>

Authorized Representative of LEA

Date

Verification Of Disposition of Data
by Authorized Representative of Provider

Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

solely for the LEA's purchase or renewal of Blackboard Mass Notification/Blackboard Connect, Blackboard Web Community Manager, Blackboard Ally, Blackboard Social Media Manager, or Blackboard Mobile Application, as applicable

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Duarte Unified School** which is dated _____ to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below and is purchasing or renewing one or more of the Services and who has accepted the Blackboard Master Agreement located at <http://agreements.blackboard.com/bbinc/blackboard-new-master-agreement-all-products.aspx> . 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 Student 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; (3) the Subscribing LEA doesn't agree to the standard Blackboard Master Agreement located at <http://agreements.blackboard.com/bbinc/blackboard-new-master-agreement-all-products.aspx>; or (4) three (3) years after the date of Provider's signature to this Form. Provider shall notify Libbi Garrett libbi.garrett@cite.org at CETPA in the event of any withdrawal of Exhibit E so that this information may be transmitted to the Alliance's users.

Provider: **Blackboard Inc.**

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: _____ Date: _____

Printed Name: _____ Title/Position: _____

**TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER
THIS SIGNED EXHIBIT TO PROVIDER.**

