WASHINGTON STUDENT DATA PRIVACY AGREEMENT

Version 1.0

Northshore School District

and

College Board

July 13, 2020

This Washington Student Data Privacy Agreement ("DPA") is entered into by and between the Northshore School District (hereinafter referred to as "LEA") and College Board (hereinafter referred to as "Provider") on July 13, 2020. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated July 13, 2020 ("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 several Washington State privacy laws, including Student User Privacy in Education Rights ("SUPER") 28A.604.010 *et seq*., as well as RCW 19.255.010 *et seq.* and RCW 42.56.590.

WHEREAS, for the purposes of this DPA, Provider is a School Official with legitimate educational interests in accessing educational records and performing Services 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", agree to allow other LEAs in Washington 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 the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SUPER and other applicable Washington 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" attached hereto:

   SpringBoard Materials and SpringBoard Professional Development

3. **Student Data to Be Provided**. In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

   Please see exhibit B

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C" attached hereto. 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 DPA 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 student-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 student's records, correct erroneous information, and procedures for the transfer of student-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 student's records held by the Provider to view or correct as necessary. In the event that a parent of a student 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 Student 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 Student Generated Content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Services.

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 unless legally prohibited.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance** LEA shall provide data to Provider for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SUPER and all other Washington privacy statutes.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under 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 its computer systems, 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, SUPER and all other Washington privacy statutes.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including Persistent Unique Identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above.

3. **Employee Obligation**. Provider shall require all officers, employees and agents (including, but not limited to, Subprocessors) who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

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

5. **Disposal of Data**. Upon request, Provider shall dispose of or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposal 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 and/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 disposal. 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 provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

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

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

    c. **Pre-termination Data Disposal Meeting.** In addition to the foregoing requirements, the LEA may request in writing that Provider participate in a meeting to discuss disposal of the Student Data prior to termination of the Service Agreement.

6. **Advertising Prohibition**. Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing,

advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or Services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

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

    a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees, contractors and/or Subprocessors 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 disposal work authorized under the Service Agreement.

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

    d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or who are authorized to access the Provider's computer systems and/or the 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. **Mobile Use of Student Data.** Provider shall ensure that any and all mobile devices of any type (including, but not limited to, laptops, tablets, and phones), which are used for access to, storage or analysis of Student Data by Provider's employees, contractors and/or Subprocessors shall be protected by industry standard encryption to prevent unauthorized access by third parties. Provider shall also implement a Bring Your Own Device

("BYOD") policy for its own employees, which requires them to use physical and technical safeguards against third party access to the device, and a copy of that BYOD policy shall be provided to LEA as part of Exhibit F to this DPA. Provider shall ensure that all contractors and/or Subprocessors implement BYOD policies, which provide for substantially the same level of security for mobile devices as are provided by Provider's BYOD policy.

f. 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. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

g. 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.

h. 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 (no less than semi-annually) conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

I. 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. In the event that the term of the Service Agreement is anticipated to be longer than two (2) years, Provider shall provide written confirmation to the LEA that a third party has conducted a risk assessment analysis of Provider's computer systems at some point during the term of the Service Agreement.

j. Compliance Audit. LEA shall have the right but shall be under no obligation to conduct audit(s), from time to time, of Provider's records concerning its compliance obligations as set forth in this Article V. Provider shall make such records and other documents available to LEA upon request.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA immediately following discovery of the incident. Provider shall follow the following process:

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

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

- **i.** The name and contact information of the reporting Provider subject to this section.
- **ii.** A list of the types of Student Data that were or are reasonably believed to have been the subject of a breach.
- **iii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
- **iv.** Whether the notification was delayed as a result of a law enforcement investigation and the law enforcement agency determined that notification would impede a criminal investigation.
- **v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

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

- **i.** Information about what the Provider 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 federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

f. Provider is prohibited from directly contacting parent, legal guardian or eligible student unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible student of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

g. In the event of a breach originating from LEA's use of the Service, Provider shall

cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI – INDEMNITY

1. Indemnity. Provider shall defend, indemnify and hold harmless the LEA, its officers, directors, employees, agents and assigns (the "Indemnitees") from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance carrier, arising out of or resulting from any third-party claim against the Indemnitees arising out of or resulting from Provider's failure to comply with any of its obligations under this DPA. Provider's duty to defend and indemnify the LEA includes any and all claims and causes of action whether based in tort, contract, statute, or equity. Provider agrees that it shall be obligated to accept any tender of defense by the LEA pursuant to this DPA and provide a full defense to the LEA so long as any potential exists for Provider to have an obligation to indemnify the LEA for any part of any potential judgment against the LEA.

Provider's defense and indemnity obligations herein are intended to provide for the broadest indemnity rights available under Washington law and shall survive the termination of this DPA. To the extent Provider's defense and indemnity obligations as set forth in this DPA conflict with the terms of the Service Agreement, the defense and indemnity provisions set forth herein shall control.

ARTICLE VII- 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 VIII: 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. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for a period of three (3) years, or so long as the Provider performs services under this Agreement, whichever shall be longer.

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 by Provider, its employees, or agents of the terms of this DPA.

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

4. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. No indemnification provisions granted by

the LEA in the Service Agreement shall be effective as to a breach of the terms of this DPA by the Provider. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

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

a. Designated Representatives

The designated representative for the LEA for this DPA is:

Name: Allen Miedema
Title: Executive Director of Technology

Contact Information:
3330 Monte Villa Parkway
Bothell, WA 98021
amiedema@nsd.org

The designated representative for the Provider for this DPA is:

Name: Jason Locke
Title: Senior DIrector Program Delivery

Contact Information:
250 Vesey Street
New York, NY 10281
jlocke@collegeboard.org

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: Matthew Griffin
Title: Deputy General Counsel

Contact Information:
250 Vesey Street
New York, NY 10281
privacy@collegeboard.org

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

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

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF WASHINGTON, 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 THE LEA IS LOCATED 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 DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

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

11. **Successors Bound**. This DPA is and shall be binding upon Provider's respective successors in interest 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 Washington Student Data Privacy Agreement as of the last day noted below.

Name of Provider College Board

DocuSigned by:

BY: Doug Waugh Date: July 13, 2020

F506040D64F640D...

Printed Name: Dough Waugh Title/Position: SpringBoard Materials and SpringBoard Professional Development

Address for Notice Purposes:

250 Vesey Street, New York, NY 10281

Name of Local Education Agency Northshore School District

BY: Date: 7.15.2020

Printed Name: Allen Miedema Title/Position: Executive Director of Technology

Address for Notice Purposes:

3330 Monte Villa Parkway
Bothell WA, 98021
amiedema@nsd.org

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. SOME COMMON EXAMPLES INCLUDE TEACHER ASSESSMENT TOOL, CLASSROOM MANAGEMENT, INTERACTIVE EDUCATIONAL GAMES, INTERACTIVE LESSON PLANNING, CLASSROOM MESSAGING APP, INTERACTIVE WHITEBOARD.]

Type of Product or Service	Name of Product or Service	Description of Product or Service
Example: Digital Curriculum	*1-2-3 Math Curriculum*	*Pre-made math lessons developed by subject matter experts for all school levels*
Please See the SpringBoard Schedule Attached		

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	x
		x
Assessment	Standardized test scores	X
	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	

Category of Data	Elements	Check if used by your system
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
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	x

Category of Data	Elements	Check if used by your system
Special Indicator	English language learner information	
	Low income status	
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	x
	Vendor/App assigned student ID number	x
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60	x

Category of Data	Elements	Check if used by your system
	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:	
Transcript	Student course grades	X
	Student course data	x
	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	

Category of Data	Elements	Check if used by your system
	specify:	
Other	Please list each additional data element used, stored or collected by your application	

No Student Data Collected at this time _____.
*Provider shall immediately notify LEA if this designation is no longer applicable.

EXHIBIT "C"

DEFINITIONS

ACPE (Association for Computer Professionals in Education): Refers to the membership organization serving educational IT professionals in the States of Oregon and Washington to promote general recognition of the role of IT professionals in educational institutions; improve network and computer services; integrate emerging technologies; encourage appropriate use of information technology for the improvement of education and support standards whereby common interchanges of electronic information can be accomplished efficiently and effectively.

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 as identified by Washington Compact Provision 28A.705.010. The categories of Educational Records under Washington law are also found in Exhibit B. For purposes of this DPA, Educational Records are referred to as Student Data.

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor 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.

Indirect Identifiers: Indirect identifiers include information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator (*e.g.*, state, county) and other descriptors.

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

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

Persistent Unique Identifiers. A long-lasting identification for digital objects, which allows for those digital objects to be located even if they are moved or removed.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or student-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in

aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

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

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, and Student Personal 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.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identities, 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 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.

Student Generated Content: The term "Student Generated Content" means materials or content created by a student 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 student content.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information

collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

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

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

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSAL OF DATA

Northshore School District (hereinafter referred to as "LEA") directs [College Board (hereinafter referred to as "Provider") to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. Unless modified by separate agreement pursuant to a pre-termination data disposal meeting as described in Article IV Section 5(c), the terms of the Disposal are set forth below:

Extent of Disposal	Disposal shall be:	____ Partial. The categories of data to be disposed of are set forth in an attachment to this Directive. ____ Complete. Disposal extends to all categories of data.
Nature of Disposal	Disposal 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 Disposal	Data shall be disposed of by the following date:	____ As soon as commercially practicable _____By (Insert Date) _____ Insert or attach special instructions

_____ _____
Authorized Representative of LEA Date

DocuSigned by:
Doug Waugh
F596040D64F640D...
07/13/2020
Verification of Disposal of Data Date
by Authorized Representative of Provider

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS
NORTHSHORE SCHOOL DISTRICT

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Northshore SD and which is dated July 13, 202 to any other LEA ("Subscribing LEA") who accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of Services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider 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 statues; (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 ACPE in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

BY: DocuSigned by College Board Doug Waugh F506040D64F640D... Date: 07/13/2020

Printed Name: Doug Waugh Title/Position: SpringBoard Materials and SpringBoard Professional Devel

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.

Insert Subscribing LEA's Name

BY: _____ Date: _____

Printed Name: _____ Title/Position _____

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

Name: Matthew Griffin

Title: Deputy General Counsel

Email Address: privacy@collegeboard.org

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

The College Board is committed to ensuring data and information security. To that end, we maintain an ISO27001 certification and SOC2/SOC3 reports which attest to our compliance with well-known and generally accepted security standards. These documents are prepared following a robust and comprehensive review by a 3rd party external auditor and we are confident that they provide the assurance you are seeking.

These documents are confidential, and access will be provided via Blackberry® WorkSpaces. WorkSpaces is a secure service that will allow a member of your team to review these documents, but no one will not be able to download or forward them. We ask that Northside School District respect the confidentiality of these documents and handle them appropriately.

Attachment A

SPRINGBOARD® SCHEDULE

1. SpringBoard Program Overview.

The SpringBoard Program, a proprietary program that helps prepare 6th through 12th grade students to succeed at college-level work, includes student and teacher editions, a website license to SpringBoard Digital, and professional learning, workshops, coaching services and institutes, that feature rigorous standards, instructional resources, and formative assessments in mathematics and/or English language arts through a web-supported, integrated program (the "SpringBoard Program"). This SpringBoard Schedule sets forth the terms and conditions for the SpringBoard Program.

2. License Grant. The following licenses are referred to herein collectively as the "Licenses".

2.1 License. The College Board hereby grants to Client a limited, non-exclusive, non-transferable, non-assignable, revocable license during the Term of this Agreement to access and use the SpringBoard website ("SpringBoard Digital") and to allow each of the participating schools (the "Schools") to use SpringBoard Digital and to use all content available on SpringBoard Digital in print or otherwise provided to Client via a College Board URL designated with the Client's name (the "SpringBoard URL"). Access to SpringBoard Digital is for the sole purpose of improving teaching and learning of students in the grades designated by Client in mathematics and/or English language arts within the Schools.

2.2 Schools' Compliance with License Terms. Client shall be responsible for the Schools' compliance with the terms of all Licenses set forth in this Section 2 (License Grant).

2.3 Access to SpringBoard. Schools will access the products (*e.g.* ELA for grade 10) licensed on SpringBoard Digital via the SpingBoard URL. Client understands and agrees that there is a risk of interruption to websites. Additionally, the website may be suspended from time to time for administrative purposes, as necessary, including but not limited to, system maintenance. The College Board may change the technical functionality of the website at any time upon notice (where reasonable) to Client to the extent necessary to address technical and other business needs of the College Board.

2.3.1 Restrictions on Use. Client shall not: (a) sell, rent, lease, loan, sublicense, disseminate, assign, reverse engineer, attempt to derive the source code of, transfer or otherwise provide access to third parties, make the website available for use by third parties or use the website for the benefit of any third party; (b) copy, reproduce, modify, adapt, translate or create any derivative works from the website; (c) remove, alter, obscure or tamper with any trademark, copyright or other proprietary markings or notices affixed to or contained within the website; or (d) encourage or permit any user or other third party to engage in any of the foregoing. Client shall be responsible for ensuring that all students and teachers comply with the terms of this Schedule. If Client violates any of the provisions hereof, the College Board shall have the right to terminate Client's right to use SpringBoard Digital, without waiver of any other remedy, whether legal or equitable.

2.4 Service Providers. The College Board maintains a relationship with and has agreements with certain vendors ("Service Provider(s)") for access to some of the services and tools offered through SpringBoard Digital. Client acknowledges and agrees that the information that is uploaded to SpringBoard Digital will be accessible to the applicable Service Provider for the sole purpose of providing those services to Client. Please be aware that any information supplied to Service Provider is subject to their security and privacy policies. The College Board encourages Client to read the policies of Service Provider because their privacy practices may differ from the College Board's practices.

3. Professional Learning. The College Board shall furnish SpringBoard professional learning, workshops, coaching services and institutes (collectively, the "Services").

3.1 SpringBoard Digital Access during Services. In connection with the Services, the College Board shall provide temporary access to applicable subject and grade levels of SpringBoard Digital for any participants who do not already have access, for a period of one hundred twenty (120) days. The College Board will grant complete

access to SpringBoard Digital when Client purchases Student Editions (print and/or digital) for the subject and grade level for which the temporary access was provided.

4. Products.
During the Term, the College Board shall furnish material for certain Services (collectively, the "Products"). Client acknowledges and agrees that the College Board shall be responsible for coordinating shipping and handling of the Products, as long as Client provides shipping information, contact name and phone number. The fees for the Products are set forth in Section 6.

5. Client Obligations.

5.1 Client shall provide certain information on the participating students in the Schools for the SpringBoard Program ("Registration Information"). Unless the College Board otherwise directs, the Registration Information shall include each student's first and last name, grade, class section (by teacher name), school and district. At no additional cost to Client, Client may use a third party to upload and manage the Registration Information for students participating in the SpringBoard Program. Client and the third party shall enter into a separate written agreement documenting this arrangement. Client may also choose to manually update the Registration Information directly on SpringBoard Digital. Client shall be solely responsible for any updates to the participating students' Registration Information after it has been imported to SpringBoard Digital.

5.2 Client shall comply with the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232g, and its implementing regulations, 34 C.F.R. pt. 99 ("FERPA") in connection with the SpringBoard Program. Client shall obtain any and all consents necessary for students to participate in the SpringBoard Program, and Client shall include in its annual notification of rights under FERPA criteria that support the designation of the College Board and its employees as school officials with legitimate educational interests. Client authorizes the College Board to use personally identifiable, non-directory information to conduct studies with the purpose of improving instruction for the SpringBoard Program in accordance with 34 C.F.R. 99.31(a)(6)(i).

5.3 Client shall notify the College Board of any changes to school participation, student edition orders and License orders, as applicable. The College Board may delay and/or withhold furnishing student editions until Client confirms the student edition order.

5.4 Workshops.

5.4.1 For any workshop presented by the College Board to a group of teachers or educators, as applicable (the "Workshop"), Client shall be responsible for confirming that the duration, scope, and dates of the Workshops are in compliance with applicable local, state, and federal statutes and regulations, applicable standards of relevant national professional associations, and applicable collective bargaining agreements.

5.4.2 Client shall choose its teachers and educators to participate in any Workshop; provided, however, Client is prohibited from selling seats to teachers and educators who do not work for Client to any Workshop without advance written consent (with email to suffice) of the College Board.

5.4.3 Workshop Checklist. Client will collect and provide the College Board with the implementation information ("Implementation Information") below at least thirty (30) days prior to the first day of the Workshop, or upon execution of this Agreement if College Board is offering an Expedited Workshop:

5.4.3.1 District Information. District contact information, District Workshop Coordinator, District contract signatory, number of participating middle schools, and/or number of participating high schools.

5.4.3.2 School Information. School contact information, principal contact information, School Workshop coordinator, and where applicable information technology contact.

5.4.3.3 Workshop Site. Venue address to host the Services, which includes a meeting room and where applicable, audio-visual equipment.

5.4.3.4 Participant Information. The number of participants, and their subject and grade levels. Client agrees that the College Board may rely on such list in determining the number of materials and consultants provided by the College Board to Client at such Service.

5.4.3.5 Particpatant Attendance. The number of participants may not exceed the maximum outlined in the Professional Learning Catalog, or Client will be subject to the Participant Fee outlined in section 6 below.

5.4.3.6 Designation of Workshop Coordinator. Client shall designate a workshop coordinator who shall be the College Board's principal contact and shall assist in the organization and training.

5.4.3.7 Information Technology Contact. Client shall designate and shall cause each School to designate an information technology contact. Client information technology contact and the School information technology contacts shall address any technical issues that may arise in the course of the Service.

5.5 Network Access and Internet Connectivity. Client will ensure network access and Internet connectivity during the Workshop and and will require Client information technology contact or another appropriate staff person to be available during the Services to assist in the maintenance of such network access and Internet connectivity.

5.6 Accommodations and Instruments. Client shall furnish workshop space, instruments such as overheads, projectors, chairs and desks, DVD player and monitor, and whiteboards as necessary for the Services, and any food or refreshments Client wishes to have onsite.

The College Board reserves the right to change the Implementation Information at any time. In the event the College Board does not timely receive the Implementation Information required Client may be subject to the expedited planning fees outlined in Section 6 below, and the College Board reserves the right to decline furnishing the Services.

Services requested less than sixty (60) days in advance of the start date shall be subject to the expedited planning fee outlined in Section 6 below. The College Board shall not accept any orders for Services scheduled less than twenty-one (21) days in advance of the start date.

If the College Board agrees to furnish Services without complete Implementation Information, then the College Board shall not be responsible if Client believes it has received incomplete or ineffective Services.

6. Fees and Payment.

6.1 Fees. The fees for Licenses and student editions shall be **$____.** The fees for the Services shall be **$____** and the Products shall be **$____**. The fees for Licenses, Services and Products shall be collectively referred to as "Fee(s)." Client agrees to pay any applicable sales, use, value added or other taxes or import duties (other than the College Board's corporate income taxes) based on, or due as a result of, any Fees paid to the College Board under this Schedule, unless Client is exempt from such taxes as the result of Client's corporate or government status. Client shall furnish the College Board with a valid tax exemption certificate. The total fee calculation for this SpringBoard Schedule as of the Effective Date of this Agreement shall be set forth in the Budget, incorporated hereto. The Fees may be based on estimated student participation figures furnished to the College Board by Client prior to the Effective Date of this Agreement and do not accommodate any orders placed thereafter.

6.1.2 Costs Excluded from Fees for Services. The Fee does not cover the following costs associated with Services: meeting room fees, audio-visual fees, food, insurance, fees for applicable substitute teachers and other costs for Client personnel, and other on-site or off-site transportation expenses and lodging. Client shall be responsible for and pay directly the costs not covered by the Fee.

6.1.2 Rescheduling Costs for Services. In addition to the full cost of the Service, for Services cancelled or rescheduled less than thirty (30) days prior to the first day of the Services, Client shall pay the

College Board a fee equal to 50% of the full cost of the Service. For Services cancelled or rescheduled less than fifteen (15) days prior to the first day of the Services, Client shall pay the College Board a fee equal to 75% of the full cost of the Services. These fees apply to all Services in this Agreement, and will be calculated on the full published rate, regardless if Client has received any discounts. The College Board retains the right, in its sole discretion, to apply these fees for rescheduling requests.

6.1.3 **Expedited Workshop Planning Fee**. If Client places an order for a Service less than sixty (60) prior to the requested date, Client shall be subject to an expedited planning fee of forty percent (40%) of the cost of such Service. Client must provide a purchase order, check, or credit card payment for processing in addition to all of the required information outlined in the Workshop Checklist (Section 5.4.3) in connection with scheduling Services less than sicty (60) days in advance. This expedited panning fee shall apply to all Services under this Schedule, regardless of whether Client has received any discounts for such Services.

6.1.4 **Participant Fee for Services**... If the number of participants present at the Service exceeds the maximum defined in the Professional Learning Catalog, Client is subject to a fee of up to 20% of the total cost of the Services. This fee applies to all Services in this Agreement, and will be calculated on the full published rate, regardless if Client has received any discounts.

6.1.5 **Shipping Fees.** Client shall pay all shipping charges including any additional fees for expedited shipping requested by Client. Client may return or exchange, at Client's expense, consumable editions which are in new condition and have not yet been used up to thirty (30) days after receipt. The College Board will issue refunds within thirty (30) upon receipt of the returned editions days for Client's that do not have an outstanding balance due.

6.2 **Changes to Student Edition/License Volumes.** If the annual volumes of Student Editions/Licenses increase or decrease by more than 5% of the projected volumes agreed to at the commencement of this Agreement, then Client shall provide the College Board with the adjusted volumes no later than April 15th of the year of annual order fulfillment.

6.2.1 If during the term of this Agreement Client determines that they have an annual increase in needed volume of Student Editions/Licenses that is less than 5%, then the additional Student Editions/Licenses ordered will be provided at the price indicated in this Agreement.

6.2.2 If, during the term of this Agreement, Client determines that they needed additional Student Editions/Licenses that is greater than 5% of their projected volumes, then Client may either: amend this Agreement to reflect the revised volumes; or purchase the additional Student Editions/Licenses at the College Board's then-current price.

6.2.3 If, during the term of this Agreement, Client determines that they have an annual decrease in needed Student Editions/Licenses volumes that is within 5% of their projected volumes, then the College Board will issue a credit for the shortfall upon the expiration of this Agreement, at which time all books delivered over the term of this Agreement will be reconciled against the volume invoiced.

6.2.4 If, during the term of this Agreement, Client determines that they have an annual decrease in needed Student Editions/Licenses volumes that is greater than 5% of their projected volumes, then the parties will amend this Agreement to reflect the revised volumes.

7. **Client Representations and Warranties.** Client represents and warrants to the College Board that:

7.1 Client has designated as "directory information" for purposes of FERPA, a student's name, grade level, the most recent educational agency or institution attended, and the other items specifically identified as directory information in 34 C.F.R. 99.3. To the extent the Registration Information includes only such directory information,

the College Board may redisclose the Registration Information in accordance with the Privacy Policy without the consent of the parent or student eighteen (18) years of age or older.

7.2 To the extent that the Registration Information or other personally identifiable information from education records of students disclosed by Client to the College Board includes information other than directory information, for purposes of FERPA the College Board and its employees and independent contractors are "school officials" whom Client has determined to have "legitimate educational interests", and Client may disclose such non-directory information to the College Board consistent with FERPA and other applicable law and policy.

8. Rights After Termination. If this Agreement is terminated for any reason, all rights granted to Client hereunder shall cease, and Client shall immediately notify all teachers and students participating in the SpringBoard Program that they may no longer use SpringBoard Digital. Upon termination of this Agreement, the College Board shall terminate Client's access to SpringBoard Digital, and any and all other systems to which Client has access under this Agreement.

Upon termination, Client shall promptly pay to the College Board all Fees and other amounts due and owing under this Agreement for the Services performed, Products furnished, and Licenses granted through the effective date of termination. If this Agreement is terminated during the Initial Term or any Renewal Term, Client shall not be entitled to a refund of any Fee paid with respect to such Initial Term or Renewal Term.

9. Confidentiality and Data Protection.

9.1 Confidentiality. All information exchanged hereunder to which either party shall have access in connection with this Agreement, including the terms of this Agreement, is confidential ("Confidential Information"), and except as otherwise expressly provided in this Agreement, neither party will authorize or permit the other party's Confidential Information to be conveyed or in any manner communicated to or made available to any third party or to be physically duplicated or reproduced or used by or for the benefit of any third party, in whole or in part; provided, however, that Confidential Information shall exclude any data or information that: (a) is publicly disclosed or expressly approved for public disclosure by the act of an authorized agent of either party; (b) becomes publicly known without breach of any confidentiality obligation; or (c) is required to be disclosed pursuant to any applicable law or regulation, government authority or duly authorized subpoena or court order, provided that the disclosing party in such event shall provide the other party with notice of such requirement as soon as practicable after such requirement becomes known to the disclosing party (and in any event before any such Confidential Information is disclosed).

9.2 Data Protection. The College Board shall take actions to ensure the security and confidentiality of Confidential Information. The College Board assures that personally identifiable data is secured and protected in a manner consistent with industry standards. The College Board shall maintain the Registration Information (defined in Section 3.1) that may be obtained pursuant to this Agreement in a secure computer environment and not copy, reproduce or transmit such data except as necessary to fulfill the purpose of the original request. The College Board has security measures in place designed to help protect against loss, misuse and alteration of the data under the College Board's control. College Board shall develop, implement, maintain and use reasonably appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all stored, managed, retained, accessed or used student records received from or on behalf of Client, State, Parents or Adult Students as determined by College Board. The College Board shall host content on SpringBoard Digital in a secure server environment that uses a firewall and other advanced technology designed to prevent interference or access from outside intruders. Where applicable, SpringBoard Digital will require unique account identifiers, usernames and passwords that must be entered each time a client or user signs on.

College Board warrants that all student records will be encrypted in transmission and storage where technically feasible and when designed as being appropriate by the College Board. If not, other security controls may be implemented to reduce risk, mitigate risk, or otherwise protect the data as determined solely by the College Board. When SpringBoard Digital is accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology protects information while in transit, using both server authentication and data encryption to help ensure that data are safe, secure and available to only authorized users.

The College Board may use de-identified data: to improve the SpringBoard Program, to demonstrate the effectiveness of the SpringBoard Program, and for research or other purposes related to developing and improving the SpringBoard Program. The College Board will share de-identified data with a third-party organization Adobe for the purpose of site analytics data. The College Board's use of such de-identified data will survive termination of this Agreement.

9.2.1 **Security Measures**. To ensure the security and confidentiality of confidential records the College Board shall designate an employee responsible for the training and compliance of all College Board employees, agents, and assigns on compliance with security and confidentiality provisions detailed in this Agreement. The College Board shall not disclose student records, except as specified under the terms of the Agreement, an Amendment or as required by law. The College Board warrants that all confidentiality requirements and security measures identified in this Agreement will be extended by contract to any and all subcontractors used by College Board, if any, to execute the terms of this Agreement. The College Board will use appropriate and reliable storage media, regularly backup student records and retain such backup copies for the duration of this Agreement as defined by the College Board. The College Board acknowledges that the College Board utilizes cloud hosting service providers throughout its infrastructure. The College Board warrants that all student records will be stored in the United States where technically feasible and reasonable as determined solely by the College Board. Client acknowledges that in some cases the College Board may not be able to restrict the location of data due to limitations within the cloud hosting service provider capabilities.

9.2.2 **Notice**. In the event of an unauthorized disclosure of student records which have been distributed or received in connection with this Agreeemnt, the following process will be implemented: Client and College Board agree to notify the other party, fully investigate the incident and fully cooperate with any investigation of the incident, implement remedial measures and respond in a timely manner. Such notification shall be promptly performed as information becomes available but not greater than thirty (30) calendar days immediately upon becoming aware of: (a) a confirmed compromise of these student records, or of (b) circumstances that could have reasonably resulted in an unauthorized access to or disclosure of these student records. Both Client and College Board acknowledge that in the event of an unauthorized disclosure computer forensics teams may require many days, weeks or even months to fully ascertain the details surrounding the disclosure which may delay prompt notification within the 30-calendar day requirement.

Where information is available, parent or adult student will be immediately notified of: (1) the nature of the unauthorized use or disclosure (e.g., security breach, nonconsensual re-disclosure, etc.); (2) the specific student records that were used or disclosed without authorization where possible; (3) what the College Board and Client have done or will do to mitigate any effects of the unauthorized use or disclosure; and (4)what corrective action the College Board and Client have taken or will take to prevent future occurrences. Except as otherwise required by law, the College Board will not provide notice of the incident directly to the parent or adult student whose student records were involved, regulatory agencies, or other entities, without prior written permission from Client.

10. **Use of Cookies**. A cookie is a small text file placed on your computer's hard drive when you visit a website. The cookie gives you a unique, random ID, and this ID enables our website(s) to readily recognize each user on a subsequent visit to the site(s). For example, a cookie may indicate the preferences you selected on a prior visit. This facilitates more efficient browsing on subsequent visits, by using your preferences to customize the content and/or layout of our site(s). The College Board may use cookies in this fashion. Visitors are free to set their Web browsers to prevent the acceptance of cookies. However, subscribers of SpringBoard Digital must enable cookies to access certain areas. Be aware that the College Board website cookies do not contain personally identifiable information. Some Service Providers use cookies on College Board site(s). The College Board has no access to or control over these cookies. This privacy statement covers the use of cookies by the College Board website(s) only and does not cover the use of cookies by any third-party providers.

11. **Content Revision.** The College Board reserves the right to update the content of SpringBoard Digital, Products, Services and deliverables. If significant revisions are made to any Product, furnished under this Agreement then Client shall receive the most recent version of the Product. This shall only apply to future years from the revision date of the Product's furnished under this Agreement.

12. **Proprietary Rights and Intellectual Property.** The College Board and its Service Providers have expended substantial time, effort, and funds to create the website(s) and SpringBoard Digital. Client acknowledges and agrees

that the College Board or College Board affiliates exclusively own the copyright to (or have been granted licenses by third parties to use) all rights, title, and interest in SpringBoard Digital and the information, data, databases, images, sound recordings, audio and visual clips, and other content (collectively, "Content") provided by the website(s). Certain materials specifically designated as belonging to another party are not owned by the College Board. No copyrighted material or other Content may be performed, distributed, downloaded, uploaded, modified, reused, reproduced, reposted, retransmitted, disseminated, sold, published, broadcast or circulated or otherwise used in any way whatsoever except as expressly stated either in such materials or in this Schedule without express written permission of the College Board or permission of the copyright owner. Any modification of the Content, or any portion thereof, or use of the Content for any other purpose constitutes an infringement of the College Board's copyrights and other proprietary rights. Use of the Content on any other website (including, without limitation, internal websites and social media sites) or other networked computer environment is prohibited without prior written permission from the College Board. **Client agrees not to reproduce, duplicate, copy, sell, resell, or exploit for any commercial purposes any portion of the SpringBoard Program, use of the SpringBoard Program, or access to the SpringBoard Program.**

Client agrees and acknowledges that Workshops and Products, including, but not limited to, training notes, and materials and booklets provided to participants, including all copies thereof, are the sole and exclusive property of the College Board. Copying, disseminating, recording or streaming, or posting any SpringBoard Program material on Client's internal or any external website, including social media sites, or creating and sharing derivative works of the materials is a breach of Client's agreement with the College Board and the College Board's intellectual property rights. Client may solely use the Products described herein for the professional development and coaching services provided by the College Board in connection with Workshop participants' knowledge and use of the SpringBoard Program.

Except for the license expressly granted herein, Client shall have no rights to or other interests in SpringBoard Digital, materials or Content. The College Board reserves all rights not explicitly granted to Client under this Schedule.

Client agrees that it shall not post any SpringBoard Program material on Client's internal or any external website and shall advise all SpringBoard Program teachers and students that posting any such material, including answers to any questions on SpringBoard Digital or in SpringBoard student or teacher editions is a violation of the College Board's copyright. Client agrees that it shall not offer for resale and shall advise its teachers and administers not to offer for resale, any used or unused SpringBoard Program material, including student or teacher editions.

Amendment to

WASHINGTON STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Between
Northshore School District
and
College Board

1. **Article V.1.a – Password** is replaced with the following:

   Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level consistent with ISO27001 certification. Provider shall only provide access to Student Data to employees, contractors and/or Subprocessors 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.

2. **Article V.1.e – Mobile Use of Student Data** is replaced with the following:

   Provider shall ensure that any and all mobile devices of any type (including, but not limited to, laptops, tablets, and phones), which are used for access to, storage or analysis of Student Data by Provider's employees, contractors and/or Subprocessors shall be protected by industry standard encryption to prevent unauthorized access by third parties. Provider shall also implement a Bring Your Own Device ("BYOD") policy for its own employees, which requires them to use physical and technical safeguards against third party access to the device. Provider shall ensure that all contractors and/or Subprocessors implement BYOD policies, which provide for substantially the same level of security for mobile devices as are provided by Provider's BYOD policy.

3. **Article V.1.h – Subprocessors Bound** is replaced with the following:

   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 (annually) conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

4. **Article V.1.i – Periodic Risk Assessment** is replaced with the following:

   Provider further acknowledges and agrees to conduct digital and physical periodic (annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. In the event that the term of the Service Agreement is anticipated to be longer than two (2) years, Provider shall provide written confirmation to the LEA that a third party has

conducted a risk assessment analysis of Provider's computer systems at some point during the term of the Service Agreement.

5. **Article V.1.j – Compliance Audit** is removed in its entirety.

6. **Article V.2.e** is replaced with the following:

   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.

7. **Article V.1.f** is removed in its entirety.

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

Name of Provider

DocuSigned by:

BY: Doug Waugh — 07/13/2020

Signature — *Date*

Doug Waugh — Vice President, SpringBoard and Pre-AP Programs

Printed Name — *Title/Position*

Name of Local Education Agency

BY: — 7-15-2020

Signature — *Date*

Allen Miedema — Executive Director of Technology

Printed Name — *Title/Position*

Note: Electronic signature not permitted