

MAINE STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Portland Public Schools, Maine

and

College Board

This Maine Student Data Privacy Agreement ("DPA") is entered into by and between the

Portland Public Schools (hereinafter referred to as "School Unit") and
College Board (hereinafter referred to as "Provider") on the date provided on the
preceding page. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the School Unit with certain digital educational services ("Services") pursuant to a contract that may be entered into between the parties for any tests in the SAT Suite of Assessments ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the School Unit may provide, documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. §1232g et. seq. (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 et. seq.; and Individuals with Disabilities Education Act ("IDEA") 20 U.S.C. § 1400 et. seq. (34 CFR Part 300); and

WHEREAS, the documents and data transferred from School Units and created by the Provider's Services are also subject to several state student privacy laws, including Maine's dissemination of student records law 20-A M.R.S. §6001; Maine Student Information Privacy Act 20-A M.R.S. §951 et. seq. ("MSIPA"); and Maine Unified Special Education Regulations ("MUSER") Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, this Agreement complies with Maine laws, and federal law; 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 school units in Maine 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 School Unit pursuant to the Service

Agreement, including compliance with all applicable federal and state privacy statutes, including FERPA, PPRA, COPPA, IDEA, MSIPA, and MUSER and other applicable Maine 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 School Unit. Provider shall be under the direct control and supervision of the School Unit with respect to the use and maintenance of information shared with Provider by School Unit pursuant to this Agreement and the Service Agreement.

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

See Attached Exhibit A

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

See Attached Exhibit A

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of School Unit** . 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 School Unit. 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 shall remain the exclusive property of the School Unit. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the School Unit 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.** School Unit shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data on the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than 30 days from the date of the request for Student Data related to regular education students; and without unnecessary delay for Student Data related to special education

students and, for such requests made in anticipation of an IEP meeting, due process hearing, or resolution session, without unnecessary delay and before any such meeting, due process hearing, or resolution session and, in either case, in no event more than 30 days from the date of the request) to the School Unit's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the School Unit, who will follow the necessary and proper procedures regarding the requested information.

Separate Account. Provider shall, at the request of the School Unit, use reasonable efforts to transfer Student Generated Content to a separate student account where not unduly burdensome.

3. **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 School Unit. Provider shall notify the School Unit in advance of a compelled disclosure to a Third Party. The Provider will not use, disclose, compile, transfer, and/or sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof.
4. **No Unauthorized Use.** Provider shall not use Student Data for any purpose other than as explicitly specified in the Service Agreement. Any use of Student Data shall comply with the terms of this DPA.
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 SCHOOL UNIT

1. **Provide Data In Compliance With FERPA.** School Unit shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, IDEA, MSIPA, and MUSER and all other Maine privacy statutes and regulations referenced or identified in this DPA.
2. **Annual Notification of Rights.** If the School Unit has a policy of disclosing education records under 34 CFR § 99.31 (a) (1), School Unit 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, and determine whether Provider qualifies as a "school official."
3. **Reasonable Precautions.** School Unit 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.** School Unit shall notify Provider promptly of any known or suspected unauthorized access. School Unit 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, IDEA, MSIPA, MUSER and all other Maine privacy statutes and regulations identified in this DPA.
2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the School Unit.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to 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 School Unit, who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.
5. **Disposition of Data.** 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 and transfer said data to School Unit or School Unit's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. 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. Disposition shall include: (1) shredding any and all hard copies of any Student Data; and (2) erasing or otherwise modifying the records to make them unreadable and indecipherable. Provider shall provide written notification to School Unit when the Student Data has been

disposed of or deleted. The duty to dispose of or delete 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 School Unit may employ a “Directive for Disposition of Data” Form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the School Unit, the Provider will immediately provide the School Unit with any specified portion of the Student Data within three (3) calendar days of receipt of said request.

6. **Advertising Prohibition**. Without limiting any other provision in this DPA, Provider is specifically prohibited from using, disclosing, 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(s) to School Unit; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service(s) to School Unit.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain commercially reasonable data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees and contractors with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records 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 and/or transfer said data to School Unit or School Unit’s designee, according to a schedule and procedure as the parties may reasonable agree upon. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
 - c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best 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 data obtained or generated pursuant to the Service Agreement in a secure

computer 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 School Unit.

- d. Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide School Unit with contact information of an employee who School Unit 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 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 periodically updated according to industry standards.
- f. Security Coordinator.** Provider shall provide the name and contact information of Provider’s Security Coordinator for the Student Data received pursuant to the Service Agreement.
- g. Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.
- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments via SOC2 Type 2 and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request from School Unit, Provider shall provide School Unit with records evidencing completion of such periodic risk assessments and documenting any identified security and privacy vulnerabilities as well as the remedial measures taken to correct them via the SOC2 Type 2 Report.
- i. Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider’s system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.
- j. Audits.** Upon receipt of a request from the School Unit, the Provider will allow the School Unit to audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof via review of the SOC2 Type 2 Report. The Provider will cooperate fully with the School Unit and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or School Unit,. Failure to cooperate shall be deemed a material breach of the Agreement.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to School Unit within a reasonable amount of time of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. Provider shall follow the following process for such notification:
- 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 School Unit subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - c. At School Unit’s discretion, the security breach notification may also include any of the following:
 - i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - d. Provider agrees to adhere to all requirements in applicable state and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized

- acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide School Unit,
- f. At the request and with the assistance of School Unit, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI- GENERAL OFFER OF 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 to any other School Unit who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.
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.
3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall dispose of and destroy all of School Unit’s data pursuant to Article IV, section 5, and Article V, section 1(b).
4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the 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 the DPA and the Service Agreement, or with any other bid/RFP, license agreement, terms of use, or privacy policy, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph, 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, facsimile 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:

The designated representative for the Provider for this Agreement is:

Leslie Davis _____
____ Director, Contracts & RFP Admin. _____
____ 250 Vesey Street, New York, NY 10281 _____
____ lware@collegeboard.org _____

[INSERT INFORMATION]

The designated representative for the School Unit for this Agreement is:

[INSERT INFORMATION]

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 MAINE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS IN CUMBERLAND COUNTY, MAINE FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.

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

[Signature Page Follows]

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

BY: _____ Date: _____

Printed Name: Jeremy Singer Title/Position: President

Address for Notice Purposes: College Board
Attn: Privacy Department
250 Vesey Street
New York, NY 10281
privacy@collegeboard.org

BY:  Date: 5/23/23

Printed Name: Courtney Graffius Title/Position: Technology Integration
Coordinator

Address for Notice Purposes: Portland Public Schools, 353 Cumberland Ave.,
Portland, ME 04101

EXHIBIT “A”

DESCRIPTION OF SERVICES

Digital SAT® Suite of Assessments including: PSAT™ 8/9, PSAT™ 10, PSAT/NMSQT®¹ and SAT® School Day. See Exhibit A-1 for details on data provided to College Board in connection with these assessments.

College Board Collection and Use of Data. LEA acknowledges and agrees that the data collected from the administration of the assessment(s) noted above is subject to College Board’s privacy policies, available at <https://privacy.collegeboard.org>.

College Board shall collect from LEA the following student data in connection with the registration of the assessments noted above, with those asterisked required for registration. LEA and College Board agree to 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”), as applicable. LEA will obtain any and all consents necessary for students to participate in the assessment(s), if any.

- *First and last name
- Middle initial
- *Date of Birth
- *Attending institution (AI Code)
- *Grade
- *Gender
- *Test administration indicator (that is, which assessment)
- *Season for testing
- Student identifier

College Board may collect additional data and information from students in connection with the assessments, all of which is optional and subject to College Board’s privacy policies. See Schedule A-1 below for more information.

For digital testing, College Board will receive certain information about the device to ensure the device is compatible and monitor the actions taken in Bluebook for test security purposes, as well as to develop and improve College Board products and services.

College Board may also collect, retain, use and share students’ personally identifiable information to perform the services related to the SAT Suite of Assessments and for the purposes outlined below.

- For SAT, State Scholarship Organizations: State affiliated scholarship organizations may receive student data for the purposes of eligibility for a scholarship or recognition program.
- For SAT, National Presidential Scholars: Eligible students are shared with the US Department of Education for purposes of the U.S. Presidential Scholars Programs.

¹ PSAT/NMSQT is a registered trademark of the College Board and National Merit Scholarship Corporation.

- For PSAT/NMSQT and PSAT10, National Recognition Programs: College Board uses student data to determine eligibility and administer its National Recognition Programs and share information with the students' high school and district about the students' recognition status.
- For PSAT/NMSQT, College Board will share scores and other information provided by students during testing with the National Merit Scholarship Corporation (NMSC) in order for NMSC to determine whether students are eligible for its National Merit Scholarship Program in accordance with the PSAT/NMSQT Student Guide and www.nationalmerit.org.
- Score Reporting to Students.
- SAT Score Sends: Students may identify institutions to receive their SAT scores. Student scores and basic demographic information sufficient for identity matching are only provided to higher education institutions and scholarship organizations when authorized by students.
- Score Report to Schools, Districts and State. Schools, Districts and the State will have access to students' assessments score(s) and data derived from the score(s).
- Accommodations: College Board uses student data to process applications for testing accommodations and to communicate with the SSD coordinator and students regarding accommodations.
- Test Security: College Board may use student data to identify and investigate potential test security incidents, and protect and enhance test security, and disclose the results of test security investigations with third parties, including to the student's school, any score recipient, college, higher education institution or agency, scholarship organization, potential score recipient government agency in the U.S or abroad, parents, legal guardians, or law enforcement.
- Research: College Board may use de-identified data obtained from student test-takers for psychometric and educational research purposes to evaluate the validity of College Board assessments and ensure that tests are unbiased in terms of race, gender, and culture. College Board may also use data to maintain, develop, support, improve and diagnose our services and applications.
- Other: College Board may disclose student data as required by law, when we believe in good faith that it's necessary to protect our rights, protect an individual's safety or the safety of others, investigate fraud, or respond to a government request.

LEA acknowledges that students may desire to continue and further develop a direct relationship beyond the administration of SAT Suite of Assessments for the purposes of students' college and career readiness by utilizing College Board's services available to all students. The terms and conditions of this DPA related to the collection, maintenance, use, and disclosure of data shall only apply to the data College Board receives in connection with the SAT Suite of Assessments which are subject to this DPA. Nothing in this DPA is intended

to diminish or interfere with student rights in their assessment data, and no provisions in this DPA are intended to address or cover data that College Board has, or may receive, for services which are outside the scope of this DPA. College Board agrees to adhere to the Data Protection, Security Measures and Notice provisions set forth in Schedule A-2.

Schedule A-1 College Board’s Mobile Application (only available for students taking the SAT, PSAT/NMSQT and PSAT 10)

College Board shall provide the following educational services to help students navigate post-secondary and career pathways and to help K-12 educators and counselors serve their students' needs (collectively, “Educational Services”). “App” refers to a College Board mobile application that students can download from the App Store to access Educational Services.

SCORE INFORMATION: In the App, students may access their scores and other score information (collectively, “Score Information”) for College Board assessments delivered pursuant to agreements that College Board has with LEA’s school, district, or state, as applicable (collectively, “Covered Assessments”).

RECOMMENDATIONS: In the App, College Board will provide students with educational information and recommendations about college and career options including, for example, postsecondary options and opportunities, career pathways, scholarships, National Recognition Program potential eligibility, financial aid and paying for college information, and opportunities to participate in College Board research studies (collectively, “Recommendations”). In providing and customizing Recommendations, College Board may use student information collected in connection with Covered Assessments and through students’ use of Educational Services.

CONNECTIONS*: Connections is a College Board program through which students are provided information about non-profit colleges, universities, scholarship organizations and other nonprofit educational organizations (“Eligible Institutions”) based on criteria provided by those Eligible Institutions, which may include student interests, demographics, assessment score ranges, students’ use of Educational Services, and other information collected by College Board during Covered Assessment(s) for which the student opts-in to Connections. The students’ interests and preferences, such as through user controls within the App, may also influence and personalize the students’ experiences within the App and the content delivered to them through Connections. Connections is entirely optional, and students must affirmatively opt-in if they wish to participate. Unless an LEA or a school directs College Board to exclude its students from Connections (as further described below), students can opt-in during Covered Assessment(s) or in the App. Students can opt-out any time, as described more fully below.

Opted-in students may receive information and messages from Eligible Institutions in the App, by hard copy mail, and by email, subject to the student providing their home address, email, and/or downloads the mobile application,

all of which data elements are optional (collectively, “Messages”). Eligible Institutions do not know the identity of a student to which they have been matched unless and until the student chooses to provide their personal information directly to the Eligible Institution, which the student can only do outside of the App and outside of the Educational Services. For example, a student may be able to link from the application to a webpage or webform hosted by that college. College Board may track students access to such links/webpages for purposes of reporting and analytics, but College Board will not disclose such information to Eligible Institutions other than in de-identified and aggregated form. **College Board never shares students’ personally identifiable information with Eligible Institutions as part of Connections.** Messages are created by Eligible Institutions and may include text, images, videos, and interactive elements. While the messages may be personalized by College Board (e.g., student name at the top of an email) through automated means, College Board does not create, edit, or approve of Messages and is not responsible for Messages.

Students who choose to opt-in to Connections can opt out at any time, for any or all Covered Assessment(s). Students can also choose to remain in Connections for any or all Covered Assessment(s) but opt-out of individual communications channels (emails, hardcopy mailings, and in-App). Students have multiple ways to opt-out, including, an opt-out feature within the App, an unsubscribe option from Connections emails, opt-out instructions included in each mailing, and by contacting College Board’s customer service.

ADDITIONAL DETAILS REGARDING EDUCATIONAL SERVICES:

There is no incremental cost for Educational Services.

College Board shall provide LEA with reporting on its students’ use of Educational Services, with the content and cadence within College Board’s sole discretion.

College Board collects certain information from students during Covered Assessments to ensure test validity and fairness, for identity matching and the purposes described above under the “College Board Collection and Use of Data” section. College Board also uses that information in Educational Services, as described above. For students who use the App, they may be able to update this information within the App, if they so choose. **All questions are optional.** More information about College Board’s Privacy Policies is located at collegeboard.org/privacycenter.

Questions include the following:

- Home/Mailing Address
- Mobile Phone Number
- Email Address
- Race
- Ethnicity
- First Language
- Best Language

- GPA
- Intended College Major
- Level of Education Aspirations
- Parents' Level of Education

The following are only asked for the PSAT/NMSQT:

- Whether the student is enrolled in high school traditional or homeschooled
- Whether the student will complete or leave high school and enroll full-time in college
- How many total years the student will spend in grades 9-12
- Whether the student is a U.S. citizen

To use the App, students provide a mobile number during the administration of the Covered Assessment and are encouraged to provide an email address solely for App account recovery purposes. By providing their mobile number, the student authorizes College Board to text them to download the App and authenticate into the App, about their scores, including when their scores are available, and with App notifications (if the student elects to turn on those notifications). The foregoing is clearly explained to the student. The student's phone number authenticates the student into the App. College Board does not use mobile numbers collected during Covered Assessments for any other purposes.

LEA may direct College Board to automatically exclude its students from Connections for one or more Covered Assessments by contacting College Board Customer Service at (866) 609-1369. LEA may visit collegeboard.org/connections-tc for more information about Connections and for access to an opt-out form.

- Opt-outs must be submitted before the Ordering Deadline for each assessment to suppress displaying the Connections opt-in to students during their testing experience for the Covered Assessment(s).
 - o If a student had already opted-in to Connections before Client opted-out of Connections for a Covered Assessment, (i) the student's data from Covered Assessment(s) for which Client opted out of Connections will no longer be used for Connections upon College Board's implementation of Client's opt out; (ii) the student's data from any Covered Assessment(s) for which Client chose *not* to opt-out of Connections may continue to be used for Connections and the student may still use the Connections feature within the App; and (iii) if Client excludes its students from Connections for *all* Covered Assessments, use of the student data for Connections for those Covered Assessments will cease upon College Board's implementation of Client's opt out, the students will not receive any new Messages, and any previously delivered Messages may be still accessed by students.
- In some instances, LEA's state may have elected to opt-out its students and College Board will abide by that exclusion for LEA's students.
- If LEA opts-out, LEA may revoke this opt-out election by contacting College Board at SAT Customer Service at 888-SAT-HELP, +1-212-520-8600 (International), or email sateducator@collegeboard.org.

- If LEA opts-out, LEA's students will not going forward be able to opt-in to Connections for the Covered Assessment(s) for which LEA opted out of Connections.
- Upon opt-out, students will still be able to use the App to receive Score Information and Recommendations, so long as the student provides their mobile number during the Covered Assessment.

Students may have opportunities to link from the App to BigFuture® and to other college and career planning services on College Board's website, www.collegeboard.org. Those services are not part of Educational Services and do not use student data collected under the assessments which are the subject matter of this DPA, the only exception being scores on College Board assessments, as all students have independent rights in their own test scores. Students use BigFuture in their personal capacity and may need a personal College Board account to use certain features. Students with personal College Board accounts may also be able to access their scores through their personal accounts. Students may also have opportunities to copy data from their personal College Board accounts to Educational Services for use by Connections. Such data copies shall be considered part of Educational Services and those copies are subject to the same privacy rules as student data collected during Covered Assessments. collegeboard.org/privacycenter.

EXHIBIT “B”

SCHEDULE OF DATA
See Schedule A

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	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	

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	
	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)	

Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	

Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	

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:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	

Category of Data	Elements	Check if used by your system
Student In App Performance	Program/application performance (typing programstudent types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	

	Student app passwords	
Student Name	First and/or Last	

Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if used by your system
	Student bus card ID number	
	Other transportation data - Please specify:	

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

EXHIBIT “C”

DEFINITIONS

METDA (Maine Educational Technology Directors Association): Refers to the membership organization serving educational IT professionals in the state of Maine 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.

Covered Information: Covered Information means materials that regard a student that are in any media or format and includes materials as identified by MSIPA. The categories of Covered Information under Maine law are found in Exhibit B. For purposes of this DPA, Covered Information is referred to as Student Data.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or school unit, 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 and 504 plans. The categories of Educational Records under Maine 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 Provider removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST 800-63-3: Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 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. This term shall encompass the term "Third Party," as it is found in applicable state statutes.

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

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

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

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by School Unit 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 School Unit employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records and Covered Information.

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

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

Subscribing School Unit: A School Unit 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 School Unit or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

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

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

("School Unit" directs

("Company") to dispose of data obtained by Company pursuant to the terms of the Service Agreement between School Unit and Company. The terms of the Disposition are set forth below:

1. Extent of Disposition

___ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

___ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

___ Disposition shall be by destruction or deletion of data.

___ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

3. Timing of Disposition

Data shall be disposed of by the following date:

___ As soon as commercially practicable

___ By

4. Signature

Authorized Representative of School Unit

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT “E”

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and College Board and which is date to any other School Unit (“Subscribing School Unit”) 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 School Unit may also agree to change the data provide by School Unit to the Provider to suit the unique needs of the School Unit. 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 the either the METDA or SDPC in the event of any withdrawal so that this information may be transmitted to the Alliance’s users.

BY: _____

Date: _____

Printed Name: Jeremy Singer

Title/Position: President

2. Subscribing School Unit

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

BY: _____

Date: _____

Printed Name: _____

Title/Positon _____

EXHIBIT “F” DATA SECURITY REQUIREMENTS

Data Protection, Security Measures and Notice

Data Protection. College Board shall take actions to protect the security and confidentiality of personally identifiable information that may be obtained in connection with assessments which are the subject matter of this DPA in a manner consistent with industry standards. College Board will maintain a SOC 2 Type 1 report.

College Board has security measures in place designed to help protect against loss, misuse and alteration of the data under 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 personally identifiable information that may be obtained in connection with assessments which are the subject matter to this DPA, as determined by College Board. College Board shall host content in a secure server environment that uses a firewall and other advanced technology designed to prevent interference or access from outside intruders. Where applicable, College Board platforms utilized in performance of this DPA will require unique account identifiers, usernames and passwords (as applicable) that must be entered each time a user signs on.

College Board encrypts personally identifiable information that may be obtained in connection with assessments which are the subject matter of this DPA in transmission and storage where technically feasible and when designed as being appropriate by College Board. If not, other security controls may be implemented to reduce risk, mitigate risk, or otherwise protect the data as determined solely by College Board. When College Board’s platforms are 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 secure the data and limit availability to only authorized users.

LEA shall be responsible for removing access to College Board’s platforms for any personnel who no longer should have access, or promptly notifying College Board to request removal of any such access.

Security Measures. College Board will extend the confidentiality requirements and security measures identified in this DPA by contract to subcontractors used by College Board, if any, to provide services related to the assessments which are the subject matter of this DPA. College Board will use appropriate and reliable storage media, regularly backup data and retain such backup copies for the duration of this DPA, as defined by College Board. LEA acknowledges that College Board utilizes cloud hosting service providers throughout its infrastructure. College Board will store personally identifiable information that may be obtained pursuant to the assessments which are the subject matter of this DPA in the United States where technically feasible and reasonable, as determined solely by College Board. LEA acknowledges that in some cases

College Board may not be able to restrict the location of data due to limitations within the cloud hosting service provider capabilities.