

## **VENDOR-SPECIFIC ('MODIFIED') STUDENT DATA PRIVACY AGREEMENT**

**(Florida National Data Privacy Agreement (NDPA) Standard VERSION 2)**

Charlotte County Public Schools

And

College Board, Inc.

**Version 2**

***Authored by Members of the Student Data Privacy Consortium (SDPC) &***

***Mark Williams, Fagen, Friedman & Fulfrost LLP***

© Access 4 Learning (A4L) Community. All Rights Reserved.

*This document may only be used by A4L Community members and may not be altered in any substantive manner.*

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "Effective Date") and is entered into by and between:

[Charlotte County Public Schools],

located at [1445 Education Way, Port Charlotte, FL, 33948] (the "LEA")

and

[College Board, Inc.],

located at [250 Vesey Street, New York, NY 10281] (the "Provider").

## PREAMBLE

**WHEREAS**, the Provider is providing educational or digital Services, as defined in Exhibit "A", to LEA, which Services may include: (a) cloud-based Services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

**WHEREAS**, the Provider and LEA have entered into a Service Agreement (as defined herein), to provide certain Services to the LEA as set forth in the Service Agreement, and this DPA (collectively the "Agreement"),

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h; and the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6506 (16 C.F.R. Part 312),

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

LEA and Provider agree to the additional terms or modifications detailed in Exhibit "H".

*Special Provisions. (Check if Required)*

- ☒ If checked, the Supplemental State Terms attached hereto as Exhibit "G" are hereby incorporated by reference into this DPA in their entirety.

*General Offer of Privacy Terms.*

- ☒ If checked, the Provider has signed Exhibit "E" to the SDPC Standard Clauses, otherwise known as "General Offer of Privacy Terms" enabling other LEAs to enter into the same terms of this DPA with Provider.



## MODIFIED STUDENT DATA PRIVACY AGREEMENT

Version 2.0

The **designated representative for the LEA** for this DPA is:

Name: Carl Hendrick Title: CTO  
 Address: 1445 Education Way, Port Charlotte, FL, 33948  
 Phone: 9412550808 Email: carl.hendrick@yourcharlotteschools.net

The **designated representative for the Provider** for this DPA is:

Name: Leslie Davis Title: Director, Contracts & RFP Administration  
 Address: 250 Vesey Street, New York, NY 10281  
 Phone: 212-713-8000 Email: contractsmanagement@collegeboard.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: [ Charlotte County Public Schools ]

Signed By:  Date: 4/23/25  
 Printed Name: Carl Hendrick Title/Position: CTO

PROVIDER: [ College Board ]

Signed By:  Date: 04/22/2025  
 Printed Name: Jeremy Singer Title/Position: President

Each Party is responsible to promptly notify the other Party of changes to the notice information.

**Notices to Provider**

[ College Board ]  
 [ Contracts Management ]  
 [ 250 Vesey Street, New York, NY 10281 ]  
 [ contractsmanagement@collegeboard.org ]

**Notices to LEA**

[ Charlotte County Public Schools ]  
 [ CTO ]  
 [ 1445 Education Way, Port Charlotte, FL, 33948 ]  
 [ Carl.Hendrick@yourcharlotteschools.net ]

With a copy to (if provided):

[ College Board Legal Counsel ]  
 [ 250 Vesey Street, New York, NY 10281 ]  
 [ privacy@collegeboard.org ]

With a copy to (if provided):

[ ]  
 [ ]  
 [ ]

**Security Notices to Provider** (Required per Section 5.3)

[ Holly Anderson ]  
 [ Sr. Director, Security Policy ]  
 [ 250 Vesey Street, New York, NY 10281 ]  
 [ handerson@collegeboard.org ]

**Security Notices to LEA** (Required per Section 5.3)

[ Kota Olivera ]  
 [ IT Security Specialist ]  
 [ 1445 Education Way, Port Charlotte, FL, 33948 ]  
 [ kota.olivera@yourcharlotteschools.net ]



## STANDARD CLAUSES

### ARTICLE I: PURPOSE AND SCOPE

#### 1.1 Purpose of DPA.

The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time. In performing the 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 its use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA as set forth in this DPA and the Service Agreement.

#### 1.2 Description of Products and Services.

A description of all products and services covered by the Agreement, and information specific to this DPA, are listed in Exhibit "A". If a Provider needs to update any information on Exhibit "A" (such as updating with new provided services), they may do so by completing the Addendum template provided by the A4L Community and sending a copy to the LEA.

Provider may add or delete products or services subject to this DPA under the following circumstances:

1. Deleted products or services: The products or services have been discontinued and are no longer available from the Provider.
2. Added products or services: The added products or services are either:
  - a. a direct replacement, or substantially equivalent to the original products or services listed in the DPA, or
  - b. the added products or services result in enriched new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed.

If an added product or service requires additional Data Elements, Provider must complete the relevant portion of the Addendum template to update Exhibit "B".

Provider may not make any change to Exhibit "A" via an Addendum, except adding or deleting products or services. LEA is under no obligation to acquire added products or services, and has no ability under the DPA to prevent deletion of products or services. Subject to the limitations in this section, an Addendum is automatically incorporated into this DPA when LEA is notified by Provider, in accordance with the notification provisions of this DPA, of the Addendum's existence and contents.

#### 1.3 Student Data to Be Provided.

In order to perform the services, the Provider shall process Student Data as identified by the Provider in the Schedule of Data, attached hereto as Exhibit "B". Student Data may be provided by the LEA or created by students, as set forth fully in the definition of Student Data in Exhibit "C". If a Provider needs to update any information on Exhibit "B", they may do so by completing the Addendum template provided by the A4L Community and sending a copy to the LEA.

Provider may delete data elements from Exhibit "B" if they are no longer used by the Provider.



Provider must add data elements to Exhibit "B", when a material change has occurred, regardless of whether the added data elements are either one of the following:

1. used to better deliver the original products or services listed in the DPA, or
2. used to deliver added products or services that result in new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed. Such new products or services must be designated in the Addendum template as changes to Exhibit "A".

The Provider must notify the LEA, in accordance with the notification provisions of this DPA, of the existence and contents of an Addendum modifying Exhibit "B". The LEA will have thirty (30) days from receipt to object to the Addendum. If no written objection is received it will become incorporated into the DPA between the parties.

#### **1.4 DPA Definitions.**

Capitalized terms used in this DPA shall have the meanings set forth in Exhibit "C". With respect to the treatment of Student Data, in the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to, the Service Agreement.

## **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

### **2.1 Student Data Property of LEA.**

As between LEA and Provider, all Student Data processed by the Provider, or created by students (as set forth fully in the definition of Student Data in Exhibit "C"), pursuant to the 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 processed by the Provider, including any modifications or additions or any portion thereof from any source, are also 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.

### **2.2 Parent, Legal Guardian and Student Access.**

The LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student (as defined in FERPA) may review Student Data and request deletion or modification, and request delivery of a copy of the Student Data. In support of this, the Provider shall establish reasonable procedures by which the LEA may access, and correct if necessary, Education Records and/or Student Data, and make a copy of the data available to the LEA or (at the LEA's direction) to the parent, legal guardian or eligible student directly. If the LEA is not able to review or update the Student Data itself, Provider shall respond in a reasonably timely manner (and no later than thirty (30) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent, legal guardian or student, whichever is sooner) to the LEA's request for Student Data held by the Provider to view or correct as necessary.

In the event that a parent or legal guardian of a student or eligible student contacts the Provider to correct, delete, review or request delivery of a copy of any of the Student Data collected by or generated through the Services, the Provider shall refer that person to the LEA, who will follow the necessary and proper procedures regarding



the requested information. In the event that any person other than those listed contacts the Provider about any Student Data, the Provider shall refer that person to the LEA, except as provided in Section 4.4.

- 2.2.1 This NDPA does not impede the ability of students to download, export, or otherwise save or maintain their own Student Generated Content directly from Provider or for Provider to provide a mechanism for such download, export, transfer or saving to students, or the student's parent or legal guardian. Nor does it impede the ability of Providers to offer LEAs features to allow such ability.
- 2.2.2 In the event that Student Generated Content is transferred to the control of the student, parent or legal guardian, the copy of such Student Generated Content that is in the control of such person is no longer considered Student Data.

### **2.3 Subprocessors.**

Provider shall enter into a Subprocessor Agreement with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA. Every Subprocessor Agreement must provide that the Subprocessor will not Sell the Student Data. The terms of a Subprocessor Agreement shall not be materially modified by the Subprocessor unless notice is provided to the Provider.

## **ARTICLE III: DUTIES OF LEA**

### **3.1 Provide Data in Compliance with Applicable Laws.**

LEA shall use the Services and provide Student Data in compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time.

### **3.2 Annual Notification of Rights.**

If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 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.

### **3.3 Reasonable Precautions.**

LEA shall employ administrative, physical, and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted Student Data from unauthorized access, disclosure, or acquisition by an unauthorized person.

### **3.4 Unauthorized Access Notification and Assistance.**

LEA shall notify Provider within seventy-two (72) hours of any confirmed Data Breach to the Services, LEA's account or any Student Data that poses a privacy or security risk. If requested by Provider, LEA will provide reasonable assistance to Provider in any efforts by Provider to investigate and respond to such Data Breach.



## ARTICLE IV: DUTIES OF PROVIDER

### 4.1 Privacy and Security Compliance.

The Provider shall comply with all laws and regulations applicable to Provider's protection of Student Data privacy and security, and at the direction of the LEA shall cooperate with any state or federal government initiated audit of the LEA's use of the Services.

### 4.2 Authorized Use.

The Student Data processed pursuant to the Services shall be used by the Provider for no purpose other than performing the Services outlined in Exhibit "A", or as instructed by the LEA.

### 4.3 Provider Employee Obligation.

Provider shall require all of Provider's employees who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee with access to Student Data pursuant to the Service Agreement.

### 4.4 No Disclosure.

Provider acknowledges and agrees that it shall not sell or disclose any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data.

#### 4.4.1 Exceptions to No Disclosure.

- 4.4.1.1 This prohibition against disclosure will not apply to Student Data where disclosure is directed or permitted by the LEA or this DPA.
- 4.4.1.2 The provision to not sell Student Data shall not apply to a Change of Control.
- 4.4.1.3 This prohibition against disclosure shall not apply to Student Data disclosed pursuant to a judicial order or lawfully issued subpoena or warrant.
- 4.4.1.4 This prohibition against disclosure shall not apply to Student Data disclosed to Subprocessors performing Services on behalf of the Provider pursuant to this DPA.
- 4.4.1.5 Should law enforcement or other government entities ("Requesting Party(ies)") provide a judicial order or lawfully issued subpoena or warrant to the Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party.
- 4.4.1.6 Notification under 4.4.1.5 is not required if the judicial order or lawfully issued subpoena or warrant states not to inform the LEA of the request.
- 4.4.1.7 Should the LEA be presented with a judicial order or lawfully issued subpoena or warrant to disclose Student Generated Content or other Student Data, the Provider shall cooperate with the LEA in delivering such data.



- 4.4.1.8 This prohibition against disclosure shall not apply to LEA-authorized users of the Services, which may include parents and legal guardians.
- 4.4.1.9 This prohibition against disclosure shall not apply to protect the safety of users or others, if and only if, an LEA employee who has specifically been authorized to declare a health or safety emergency has done so and all requirements under 34 CFR §§ 99.31(a)(10) and 99.36 have been fulfilled by the LEA.
- 4.4.1.10 This prohibition against disclosure shall not apply to protect the integrity or security of the Service, where such disclosure is made to a Subprocessor engaged by Provider for the specific purpose of investigating a potential Data Breach as set forth in 5.4.

## 4.5 De-Identified Data

Provider agrees not to attempt to re-identify De-Identified Student Data without the written direction of the LEA. De-Identified Student Data may be used by the Provider for those purposes allowed under applicable laws, for the purposes allowed for the processing of Student Data under this DPA, as well as the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) research, development, and improvement of the Provider's educational sites, Services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Student Data shall survive termination of this DPA or any request by LEA to return or dispose of Student Data. Except for Subprocessors, Provider agrees not to transfer De-identified Student Data to any third party unless the transfer is expressly directed or permitted by the LEA or this DPA. Such Subprocessors must be subject to equivalent terms of the DPA including this one. Prior to publishing any document that names the LEA, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Student Data is presented. If Provider chooses to create De-Identified Data, its process must comply with either NIST de-identification standards or US Department of Education guidance on de-identification.

## 4.6 Disposition of Data.

Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree.

If the Provider has a standard retention and destruction schedule, that schedule shall apply to Student Data as long as this DPA is active. The Provider's practice relating to retention and disposition of Student Data shall be provided to the LEA upon request.

At the termination of this DPA, the Provider shall, unless directed otherwise by the LEA, dispose of, or delete Student Data obtained by the Provider under the Agreement within sixty (60) days of termination (unless otherwise required by law). If the Agreement has lapsed or is not terminated, the Student Data shall be deleted when directed or permitted by the LEA, according to Provider's standard destruction schedule, or as otherwise required by law. The LEA may provide the Provider with special instructions for the disposition of the Student Data, by transmitting to Provider Exhibit "D", attached hereto. The duty of the Provider to dispose of or delete Student Data shall not extend to De-Identified Data or to Student-Generated Content that has been transferred or kept pursuant to Section 2.2.2.



#### **4.7 Advertising Limits.**

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA; or (c) for any commercial purpose other than to provide the Service to the LEA, or as authorized by the LEA or the parent/guardian. Targeted Advertising is strictly prohibited. However, this section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to account holders that are not considered Targeted Advertising (this exception does not apply where the Provider is relying on the LEA to provide consent on behalf of the parent under COPPA); or (iii) to notify account holders about new education product updates, features, or Services that are not considered Targeted Advertising or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

Before making product recommendations under section (ii) above, Provider must disclose the existence of those recommendations to LEA in writing, in sufficient detail that LEA can fulfill any obligations under applicable law (e.g. PPRa).

### **ARTICLE V: DATA SECURITY AND BREACH PROVISIONS**

#### **5.1 Data Storage.**

If Student Data is stored outside the United States, Provider will provide a list of Countries where data is stored, in Exhibit "B".

#### **5.2 Security Audits.**

Provider will conduct a security audit or assessment no less than once per year, and upon a Data Breach. Upon 10 days' notice and execution of confidentiality agreement, Provider will provide the LEA with a copy of the audit report, subject to reasonable and appropriate redaction.

#### **5.3 Data Security.**

The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security of Student Data. The Provider shall implement an adequate Cybersecurity Framework that incorporates one or more of the nationally or internationally recognized standards set forth in Exhibit "F". Additionally, Provider may choose to further detail its security programs and measures in Exhibit "F". Provider shall provide, in the Preamble to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

#### **5.4 Data Breach.**

In the event that Provider confirms a Data Breach, the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the Data Breach, unless notification within these time limits would disrupt investigation of the Data Breach by law enforcement. In such an event, notification shall be made within a reasonable time after the Data Breach. Provider shall follow the following process:



- (1) The Data Breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
  - (a) The name and contact information of the Provider subject to this section,
  - (b) the date of the notice,
  - (c) the date of the Data Breach, the estimated date of the Data Breach, or the date range within which the Data Breach occurred,
  - (d) Whether the notification was delayed as a result of a law enforcement investigation, if legally permissible to share that information,
  - (e) A general description of the Data Breach, if that information is possible to determine at the time the notice is provided,
  - (f) A description of the Student Data reasonably believed to have been the subject of the Data Breach; and
  - (g) Identification of impacted individuals.
- (2) Provider agrees to adhere to all applicable federal and state laws with respect to a Data Breach related to the Student Data, including any required responsibilities and procedures for notification and mitigation of any such Data Breach.
- (3) Provider further acknowledges and agrees to have a written Data Breach response plan that is consistent with applicable industry standards and federal and state law for responding to a Data Breach, involving Student Data and agrees to provide LEA, upon reasonable written request, with a summary of said written Data Breach response plan.
- (4) LEA shall provide notice and facts surrounding the Data Breach to the affected students, parents, or guardians.
- (5) In the event of a Data Breach originating from LEA's use of the Service or otherwise a result of LEA's actions or inactions, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data and may request costs incurred as a result of such Data Breach.



## CONTRACT TERMS

**Term and Termination.** In the event that either Party seeks to terminate this DPA, they may do so by written notice if the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any Service Agreement or contract if the other party breaches any terms of this DPA. This DPA shall stay in effect for as long as the Provider retains the Student Data, as set forth in section Article IV, Section 4.6. In the case of a "Change of Control" the LEA has the authority to terminate the DPA if it reasonably believes that the successor cannot uphold the terms and conditions herein or having a contract with the successor would violate the LEA's policies or state or federal law.

**Data Disposition on Service Agreement Termination.** If the Service Agreement is terminated, the Provider shall dispose of all of LEA's Student Data pursuant to Article IV, Section 4.6 of the Standard Clauses.

**Notices.** All notices or other communication required or permitted to be given hereunder must be made in writing and may be given via e-mail transmission, or first-class mail, or mutually agreed upon method sent to the designated representatives documented in the Preamble.

**Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. With respect to the treatment of Student Data only, in the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit "H", the SDPC Standard Clauses, and/or the Supplemental State Terms in Exhibit "G", Exhibit "H" will control, followed by Exhibit "G". Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

**Entire Agreement.** This DPA and the Service Agreement ("the Agreement") constitute 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.

**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.

**Governing Law; Venue and Jurisdiction.** This DPA will be governed by and construed in accordance with the laws of the state of the LEA, 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 of the LEA for any dispute arising out of or relating to this DPA or the transactions contemplated hereby.

**Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a Change of Control. In the event of a Change of Control, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of such Change of Control. Such notice shall include



a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement.

**Authority.** Each signatory confirms they are authorized to bind their institution to this DPA in its entirety.

**Waiver.** No delay or omission by either party to exercise any right here under shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.



## EXHIBIT A: PRODUCTS AND SERVICES

This DPA covers access to and use of [College Board]s existing Services that collect, process, or transmit Student Data, as identified below:

College Board shall provide LEA with one or more of its SAT® Suite of Assessments, which includes the PSAT™ 8/9, PSAT™ 10, PSAT/NMSQT® and SAT®, and which shall be given in a digital format on College Board's proprietary platform, Bluebook™. Data collected under this DPA shall be used to register, administer and process the assessments, which are the subject of Service Agreement entered into between the LEA and College Board, and shall solely be used as set forth in Attachment 1 of this DPA, incorporated herein by reference.



## EXHIBIT B: SCHEDULE OF STUDENT DATA

All Data Elements identified in this Exhibit are correct at time of signature.

Data Elements Collected by Product (required and optional):

Please note that LEA *may* provide the following elements in order for College Board to provide students with accommodations: English language learner information, student disability information, and specialized education services (IEP or 504). LEA *may* also choose to provide a Local (School district) ID number and the middle initial of their students. For more details on the context in which the data points indicated below are collected and whether data points are optional or required, please refer to the following sections of Attachment 1: "College Board Collection, Use, and Disclosure of Data" and "College Board's College and Career Readiness Educational Services – Additional details regarding educational services."

The product for the Data Elements selected below is the SAT Suite of Assessments and related services, including Educational Services, as defined in Attachment 1.

Category of Data / Data Elements	Enter product (s) name	Enter product (s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name
<b>Application Technology MetaData</b>							
IP Addresses of users, use of cookies, etc.	X						
Other application technology metadata	X						
If 'Other' checked, please specify below checked box:	Device Data and Activity Data. See <a href="https://bluebook.collegeboard.org/students/privacy-policy-use-bluebook">https://bluebook.collegeboard.org/students/privacy-policy-use-bluebook</a>						
<b>Application Use Statistics</b>							
Meta data on user interaction with application							
<b>Assessment</b>							
Standardized test scores	X						
Observation data							
Voice recordings							



Other assessment data	X						
If 'Other' checked, please specify below checked box:	Test administration indicator (that is, which assessment)  Season for testing						
<b>Attendance</b>							
Student school (daily) attendance data							



Category of Data / Data Elements	SAT Suite	Enter product (s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name
Student class attendance data							
<b>Communication</b>							
Online communication captured (emails, blogentries)							
<b>Conduct</b>							
Conduct or behavioral data							
<b>Demographics</b>							
Data of birth	X						
Place of birth							
Gender	X						
Ethnicity or race.	X						
Language information (native, or primary language spoken by student)	X						
Other demographic information	X						
If 'Other' checked, please specify below checked box:	GPA						
<b>Enrollment</b>							
Student school enrollment	X						
Student grade level	X						
Homeroom							
Guidance counselor							
Specific curriculum programs							
Year of graduation							

Category of Data / Data Elements	SAT Suite	Enter product (s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name
Other enrollment information							
If 'Other' checked, please specify below checked box:							
<b>Parent/Guardian Contact Information</b>							
Address							
Email							
Phone							
<b>Parent/Guardian ID</b>							
Parent ID number (created to link parents to students)							
<b>Parent/Guardian Name</b>							
First and/or last							
<b>Schedule</b>							
Student scheduled courses							
Teacher names							
<b>Special Indicator</b>							
English language learner information	X						
Low-income status							
Medical alerts/health data							
Student disability information	X						
Specialized education Services (IEP or 504)	X						
Living situations (homeless/foster care)							
Other indicator information							



Category of Data / Data Elements	SAT Suite	Enter product (s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name	Enter product(s) name
If 'Other' checked, please specify below checked box:							
<b>Student Contact Information</b>							
Address	X						
Email	X						
Phone	X						
<b>Student Identifiers</b>							
Local (school district) ID number	X						
State ID number							
Provider/app assigned student ID number							
Student app username							
Student app passwords							
<b>Student Name</b>							
First and/or last	X						
<b>Student In App Performance</b>							
Program/application performance (e.g. typing program – student types 60 wpm, reading program – student reads below grade level)							
<b>Student Program Membership</b>							
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							
<i>If 'Other' checked, please specify below checked box:</i>							
Transcript							
Student course grades							
Student course data							
Student course grades/performance scores							
Other transcript data							
<i>If 'Other' checked, please specify below checked box:</i>							
Transportation							
Student bus assignment							
Student pick up and/or drop off location							
Student bus card ID number							
Other transportation data							



If 'Other' checked, please specify below checked box:						
<b>Other</b>						
Other data collected	<b>X</b>					
If 'Other' checked, please list each additional data element used, stored, or collected by your application below checked box:	<ul style="list-style-type: none"> <li>• Testing institution</li> <li>• Registration number</li> <li>• SSD (Services for students with disabilities) ID number</li> <li>• Student Middle Initial</li> <li>• Intended College Major</li> <li>• Level of Education Aspirations</li> <li>• Parents' Level of Education</li> </ul> <p>Specifically, for PSAT/NMSQT:</p> <ul style="list-style-type: none"> <li>• Whether the student is enrolled in high school traditional or homeschooled</li> <li>• Whether the student will complete or</li> </ul>					

	<p>leave high school and enroll full-time in college</p> <ul style="list-style-type: none"> <li>• How many total years the student will spend in grades 9-12</li> <li>• Whether the student is a U.S. citizen (for students testing outside the United States)</li> </ul> <p>Specifically, for customization in the BigFuture School app and Connections:</p> <ul style="list-style-type: none"> <li>• Students' interests and preferences (such as through user controls within the BigFuture School app, through engagement in BigFuture School, and any updates students make to their information)</li> </ul>					
None						



No student data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.							
---	--	--	--	--	--	--	--

If Student Data is stored outside the United States, Provider shall list below the Countries where data is stored:

## EXHIBIT C: DEFINITIONS

**Change of Control:** Any merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of Provider or of the portion of Provider that performs the Services in the Service Agreement.

**Contextual Advertising:** Contextual advertising is the delivery of advertisements based upon a current visit to a Web page or a single search query, without the collection and retention of data about the consumer's online activities over time.

**De-Identified Data:** Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific student, including, but not limited to, any information that, alone or in combination is linkable to a specific student.

**Data Breach:** An unauthorized release, access to, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider in violation of applicable state or federal law.

**Educational Records:** Educational Records shall have the meaning set forth under FERPA 20 U.S. C. 12 32 g(a)(5)(A). For additional context see also the 'Student Data' definition.

**LEA:** For the purpose of this DPA, the LEA is the educational entity that is a Party to this Agreement. An LEA can be a state agency, an educational service agency, a charter school or school system or a private school or school system, in addition to the federal definition of Local Education Agency (LEA).

**Metadata:** Means information that provides meaning and context to other data being collected including, but not limited to date and time records and purpose of creation. Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information or Student Data.

**Originating LEA:** An educational entity otherwise meeting the definition of LEA that originally executes the DPA in its entirety (including the marked checkbox enabling Exhibit "E") with the Provider.

**School Official:** For the purposes of this DPA and pursuant to FERPA 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 Student Data including Educational Records; and (3) Is subject to FERPA 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Educational Records.

**Service Agreement:** Refers to the quote, corresponding contract, purchase order or terms of service and/or terms of use.

**Student Data:** Student Data includes any data, whether gathered, created or inferred by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose, that is descriptive of the student including, but not limited to, information in the student's Educational Record, persistent unique identifiers, or any other information or identification number that would provide information about a specific student. Student Data includes Metadata that has not been stripped of all direct and indirect identifiers. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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 include properly De- Identified Data or anonymous usage data regarding a student's or LEA's use of Provider's Services.

**Student Generated Content:** The term "Student Generated Content" means materials or content created by a student in the services 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 Generated Content" does not include student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment.

**Subprocessor:** For the purposes of this DPA, 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 service, and who has access to or storage of Student Data, including security, storage, analytics, and other processing activities necessary to perform a Provider business purpose.

**Subprocessor Agreement:** An agreement between Provider and a third party Subprocessor. A Subprocessor Agreement includes either a written agreement or an acceptance of terms and conditions (e.g., click through agreements).

**Subscribing LEA:** An educational entity otherwise meeting the definition of LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms by executing Exhibit "E".

**Targeted Advertising:** Targeted Advertising means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the Provider Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include Contextual Advertising.

## EXHIBIT D: SPECIAL INSTRUCTIONS FOR DISPOSITION OF DATA

After this DPA takes effect, if the LEA has special requirements for the disposition of Student Data that are not expressed in 4.6 Disposition of Data, the LEA may fill in this form and deliver it to the Provider.

**The Provider and the LEA must not fill in this form at the initiation of the DPA.**

The Provider shall act on Exhibit "D" from the designated representative of the LEA or their designee (Preamble or Exhibit "E" for Subscribing LEA).

Charlotte County Public Schools ("LEA") instructs Provider to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

### 1. Extent of Disposition

- ☐ Disposition is partial. The scope of Student Data to be disposed of is set forth below or found in an attachment to this Directive:  
 Insert categories of Student Data here
- ☐ Disposition is complete. Disposition extends to all Student Data.

### 2. Nature of Disposition

- ☐ Disposition shall be by destruction or deletion of Student Data.
- ☐ Disposition shall be by a transfer of Student Data. The Student Data shall be transferred to the following site as follows:  
 Insert of attach special instructions

### 3. Timing of Disposition

Student Data shall be disposed of by the following date:

- ☐ As soon as commercially practicable
- ☐ On Provider's standard destruction schedule
- ☐ By Insert Date

### 4. De-Identified Data

- ☐ The Provider certifies that they have De-Identified the data, as defined elsewhere in this Agreement, and disposed of all copies of Student Data that were not De-Identified in accordance with this Schedule and the DPA. The Provider will notify LEA in accordance with the notification requirements of the DPA using this form.  
 As of Enter Date

### 5. Other:

Signature(s)

Notice of Verified Disposition of Data

\_\_\_\_\_  
 Authorized Representative of  
 LEA

\_\_\_\_\_  
 Date

\_\_\_\_\_  
 Authorized Representative of  
 Provider

\_\_\_\_\_  
 Date



**EXHIBIT E: GENERAL OFFERS OF TERMS****Page 1 of 2: OFFER OF TERMS**

Provider and the Subscribing LEA (named below) agree by signing this General Offer of Privacy Terms ("General Offer") that they are bound by the same terms as the DPA between Provider and Charlotte County Public Schools ("Originating LEA") dated                     .

Provider and Subscribing LEA agree that the information below will be replaced throughout the DPA with the information specific to the Subscribing LEA filled in below for the Subscribing LEA. This General Offer shall extend only to the terms set forth in this DPA and shall not necessarily bind Provider or Subscribing LEA to any other terms entered into between Provider and Originating LEA. Any commercial terms, such as price, term, or schedule of Services, relating to Subscribing LEA's use of the Provider's Services shall be determined solely between Provider and Subscribing LEA.

If Provider makes changes to Exhibit "A" or Exhibit "B" in accordance with sections 1.2 and 1.3 respectively, Provider must complete the Addendum template provided by the A4L Community and notify the Originating LEA and all Subscribing LEAs in accordance with the notification provisions of this DPA, of the Addendum's existence and contents. With regard to a Subscribing LEA, an Addendum is automatically incorporated into this DPA when Subscribing LEA is notified by Provider. If an Addendum modifies Exhibit "B", the LEA will have thirty (30) days from receipt to object. If no written objection is received it will become incorporated into the DPA between the parties.

The Provider may withdraw the General Offer (for future use or for LEAs that have not already accepted it) in the event of: (1) a material change in the applicable privacy statutes; or (2) a material change in the Services and products listed in the Service Agreement. Notification of a withdrawal shall be submitted to [ndpa\\_requests@A4L.org](mailto:ndpa_requests@A4L.org).

Subscribing LEAs shall send the signed Exhibit "E" to Provider at the following email address: contractsmanagement@collegeboard.org

The below signatory confirms they are authorized to bind their institution to this DPA as in its entirety.

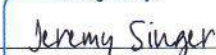
**RESOURCE NAME(S):**

[  
[  
[  
[

**PROVIDER:** [College Board ]

Signed By:

DocuSigned by:



Date:

04/22/2025

Printed Name:

BE2EE27F2DE045D...  
Jeremy Singer

Title/Position: President

**Exhibit "E" (continued)**Originating LEA: Charlotte County Public Schools

Resource Names: \_\_\_\_\_

Provider Name: College Board**Page 2 of 2: Insert Name of 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 for the term of the DPA between the Originating LEA and the Provider. **\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER.\*\***

Please note, by signing this Exhibit you are also agreeing to any language that may be included in Exhibits to the Originating DPA beyond this Exhibit "E". The below signatory confirms they are authorized to bind their institution to this DPA as in its entirety.

Subscribing LEA: Insert Name of Subscribing LEA \_\_\_\_\_

Signed By: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

School District Name: \_\_\_\_\_

**Designated Representative of LEA:**

Name: \_\_\_\_\_ Title: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Email: \_\_\_\_\_

**Notices to Subscribing LEA:** The Provider and Subscribing LEA are each responsible to promptly notify the other Party of changes to the notice information.

**Security Notices to Subscribing LEA**

[ LEA Security Name ]  
 [ LEA Security Role ]  
 [ LEA Security Postal Address ]  
 [ LEA Security Email Address ]

[ LEA Name ]  
 [ LEA Role ]  
 [ Subscribing LEA Address ]  
 [ Subscribing LEA Email Address ]

With a copy to (if provided):

LEA Legal Counsel ]  
 LEA Legal Counsel Postal Address ]  
 LEA Legal Email Address ]



## EXHIBIT F: ADEQUATE CYBERSECURITY FRAMEWORKS

Provider must mark one or more frameworks with which it complies.

The Provider may change which framework it complies with without invalidating or changing the DPA, but must notify the LEA of such change in accordance with the notification requirements of the DPA.

FRAMEWORK(S)	
	Global Education Security Standard - <a href="https://sdpc.a4l.org/gess/">https://sdpc.a4l.org/gess/</a>
	NIST Cybersecurity Framework (CSF)
	NIST SP 800-53 Security and Privacy Controls for Information systems and organizations
	NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
X	ISO 27000 series, Standards for implementing organization security and management practices
X	CIS Center for Internet Security Critical Security Controls
	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

This space is provided for optional security programs and measures as noted in section 5.3:

With respect to the boxes checked above, College Board, Inc. aligns with the NIST Cybersecurity Framework; is ISO27001 and SOC2 Type 2 certified; and is compliant with CIS level one and partially compliant for CIS level two.

## EXHIBIT G: Supplemental SDPC State Terms for Florida

Providers/Operators are to comply with the Florida Student Online Personal Information Protection Act, Florida Statute 1006.1494. This Act (effective 7/1/2023 and initiated from SB 662 in 2023) establishes new and different terms than those outlined in the National Student Data Privacy Agreement contained herein. Providers/Operators are subject to all of the Act's privacy terms, including, but not limited to the following:

**1. An operator may not knowingly do any of the following:**

- a. Engage in targeted advertising on the operator's site, service, or application, or targeted advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, which the operator has acquired because of the use of that operator's site, service or application for K-12 school purposes.
- b. Use covered information, including persistent unique identifiers, created, or gathered by the operator's site service, or application to amass a profile of a student, except in furtherance of k-12 school purposes.
- c. Share, sell, or rent a student's information, including covered information

**2. An operator shall do all the following:**

- a. Collect no more covered information that is reasonably necessary to operate an Internet website, online service, online application, or mobile application.
- b. Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information which are designed to protect it from unauthorized access destruction, use, modification, or disclosure.
- c. Unless a parent or guardian expressly consents to the operator retaining a student's covered information, delete the covered information at the conclusion of the course, or corresponding program and no later than 90 days after a student is no longer enrolled in a school within the district, upon notice by the school district.



## EXHIBIT H: DESCRIPTION OF 'AGREED TO' CHANGES

LEA and Provider agree to the following additional or replacement terms and modifications:

*The following clause in Exhibit G: Supplemental SDPC State Terms for Florida shall now state:*

**1. An operator may not knowingly do any of the following:**

- a. Engage in targeted advertising on the operator's site, service, or application, or targeted advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, which the operator has acquired because of the use of that operator's site, service or application for K-12 school purposes.
- b. Use covered information, including persistent unique identifiers, created, or gathered by the operator's site service, or application to amass a profile of a student, except in furtherance of k-12 school purposes.
- c. Share, sell, or rent a student's information, including covered information. **This paragraph does not apply to the purchase, merger, or other acquisition of an operator by a third party, if the third party complies with this section regarding previously acquired student information, or to a national assessment provider if the provider obtains the express written consent of the parent or student, given in response to clear and conspicuous notice, solely to provide access to employment, educational scholarships or financial aid, or postsecondary educational opportunities.**

*The following clause in the Preamble shall now state:*

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 C.F.R. Part 99); ~~the Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h; and the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6506 (16 C.F.R. Part 312);~~

*Article IV.4.3 shall now state:*

**Provider Employee Obligation.**

Provider shall require all of Provider's employees who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee with access to Student Data pursuant to the Service Agreement **or require such employees to agree to be bound by confidentiality provisions that are equally as restrictive as those set forth in this DPA.**

*Article IV, 4.6 shall now state:*

**Disposition of Data.**

Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree.

If the Provider has a standard retention and destruction schedule, that schedule shall apply to Student Data as long as this DPA is active. The Provider's practice relating to retention and disposition of Student Data shall be provided to the LEA upon request.

## MODIFIED STUDENT DATA PRIVACY AGREEMENT

Version 2.0

**Except as provided herein,** at the termination of this DPA, the Provider shall, unless directed otherwise by the LEA, dispose of, or delete Student Data obtained by the Provider under the Agreement within sixty (60) days of termination (unless otherwise required by law). If the Agreement has lapsed or is not terminated, the Student Data shall be deleted when directed or permitted by the LEA, according to Provider's standard destruction schedule, or as otherwise required by law. The LEA may provide the Provider with special instructions for the disposition of the Student Data, by transmitting to Provider Exhibit "D", attached hereto. The duty of the Provider to dispose of or delete Student Data shall not extend to De-Identified Data or to Student-Generated Content that has been transferred or kept pursuant to Section 2.2.2.

*Article V.5.2 shall now state:*

**Security Audits.**

Provider will conduct a security audit or assessment no less than once per year, ~~and upon a Data Breach~~. Upon 10 days' notice and execution of confidentiality agreement, Provider will provide the LEA with a copy of the audit report, subject to reasonable and appropriate redaction.

*Article V 5.4(3) shall now state:*

**Data Breach.**

Provider further acknowledges and agrees to have a written Data Breach response plan that is consistent with applicable industry standards and federal and state law for responding to a Data Breach, involving Student Data and agrees to provide LEA, upon reasonable written request, with **a copy of its SOC 2 Type II report. a summary of said written Data Breach response plan.**



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

College Board Collection, Use, and Disclosure of Data. District, School, LEA, SEA, State (each a “Client”, as applicable for which entity is entering into an agreement with College Board to obtain one or more of the tests in the SAT Suite of Assessments (“Agreement”), each a “Covered Assessment”) acknowledges and agrees that the data collected in connection with the Covered Assessment(s) and the Educational Services (defined below) is subject to the terms below, which are further described within College Board’s privacy policies, available at <https://privacy.collegeboard.org>.

College Board shall collect from Client the following student data in connection with the registration of the assessments noted above, with those asterisked required for registration. Client 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. Client 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 and name)
- \*Testing institution (AI Code and name)
- \*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 below for more information.

For digital testing, College Board will receive certain information about the device used by the student and monitor and capture actions students take when using Bluebook to ensure the device is compatible and for test security purposes, for test validation and research, as well as to develop and improve College Board products



and services. We may disclose this information but only in aggregated and de-identified form.

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

- *For SAT, State Scholarship Organizations:* State affiliated scholarship organizations may receive student data, including SAT scores(s), solely for the purposes of eligibility for a scholarship or recognition program. College Board will enter into an agreement with any such state agency for these purposes. College Board is not involved in setting the criteria for any state scholarship programs nor awarding decisions.
- *For SAT, State Direct Admissions Programs:* State government agencies that are operating direct admissions programs on behalf of their state public higher education institutions may receive student data, including SAT score(s), solely for the purposes of facilitating and administering direct admissions on behalf of those institutions. College Board will enter into an agreement with any such state agency for these purposes. College Board is not involved in setting the criteria for any direct admission programs or offers, nor is College Board involved in any decision by the state agency or the state public higher education institution(s) to make (or decline to make) any direct admission offers.
- *For SAT, National Presidential Scholars:* Data about eligible students are shared with the US Department of Education for purposes of the U.S. Presidential Scholars Programs. College Board will enter into an agreement with the US Department of Education for these purposes.
- *For PSAT/NMSQT and PSAT10, National Recognition Programs:* College Board uses student data to determine a student's eligibility to apply for or receive its National Recognition Programs award(s), for administration of the National Recognition Program, and share information with the student and their high school and district about the students' eligibility and recognition status.
- *For PSAT/NMSQT,* College Board will share scores, data derived from scores, certain student demographic information, 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 and administer this program in accordance with the PSAT/NMSQT Student Guide and [www.nationalmerit.org](http://www.nationalmerit.org). This includes NMSC sharing information with the student and their high school about the students' eligibility and recognition status.
- *Score Reporting to Students:* College Board will report to the student the score achieved on the Covered Assessment(s), insights from those scores, and their AP Potential.
- *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, including through College Board's online reporting portals, to students' assessments score(s) and data derived from the score(s) the student received on past and future College Board assessments, consistent with disclosures to the students.
- *Accommodations:* College Board uses student data to process applications for testing accommodations



the SAT School Day, PSAT/NMSQT, PSAT 10 and PSAT 8/9. "BigFuture School" as used herein refers to the Educational Services provided on the App (including in-App notifications if the student elects to turn on those notifications) and potential other channels such as through a website portal exclusively for the Educational Services.

**SCORE INFORMATION:** In BigFuture School, students may access their scores and other score information (collectively, "Score Information") for College Board assessments including scores received by students on Covered Assessments. For SAT School Day, Score Information will include career readiness indicator(s) derived from the student's scores and the U.S. Department of Labor/Employment and Training Administration Occupational Information Network (O\*NET), mapping the math, reading, and writing skills measured by the SAT to the qualitative and literacy skills for occupations in O\*NET.

**RECOMMENDATIONS:** In BigFuture School, College Board may provide students with educational information and recommendations about college and career options including, for example, AP Potential, 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 score ranges, career readiness indicators as provided in their Score Information for SAT School Day, and student information collected in connection with Covered Assessments and through students' use of Educational Services. In the Recommendations, College Board may include third-party links to other sites that are not operated by us, including colleges, universities, scholarship organizations, and career information sites. College Board is not responsible for the content or operation of other websites, and links to other websites are not intended to imply endorsement of them by College Board.

**CONNECTIONS\*:** Connections is available to students taking the SAT School Day, PSAT/NMSQT, and PSAT 10. Connections is a College Board program through which students are provided information about non-profit colleges, universities, nonprofit scholarship providers, and other government agencies administering educational programs ("Eligible Institutions") and may receive preliminary offers of admission from nonprofit colleges and universities ("Participating Colleges"). Information provided to students is based on criteria provided by those Eligible Institutions and Participating Colleges and student information and interests. This may include:

- student interests, demographics, students' use of Educational Services, and other information collected by College Board during Covered Assessment(s) for which the student opts-in to Connections;
- students' interests and preferences (such as through user controls within the App, through engagement in BigFuture School, and any updates students make to their information in their use of Educational Services);
- assessment score ranges the student received on past and future SAT, AP, PSAT/NMSQT and PSAT10 assessments; and
- for preliminary offers of admission from Participating Colleges, assessment score ranges the student received on past and future SAT assessments may be used, and race and ethnicity will not be used.



**College Board never shares students' personally identifiable information with Eligible Institutions or Participating Colleges as part of Connections.**

Connections is entirely optional, and students must affirmatively opt-in and agree to College Board's use of their information as described above for Connections 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 and may be able to do so through other channels. If a student opted-in to Connections during a prior SAT School Day, PSAT/NMSQT, or PSAT 10 assessment pursuant to an agreement with their school, district, or state, Client acknowledges and agrees to use of the student's information from Covered Assessment(s) under this Agreement in Connections, with notice of the same and opportunity to opt-out presented to any such students during the Covered Assessment(s).

Students can opt-out of Connections at any time using any of the multiple ways provided, 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. Students can also choose to remain in Connections but opt-out of individual communications channels (emails, hardcopy mailings, and in-App).

Opted-in students may receive information from and about Eligible Institutions and Participating Colleges in the App (including in-App notifications if the student elects to turn on those notifications), by hard copy mail, and by email, subject to the student providing their home address, email, and/or downloading the mobile application, all of which data elements are optional. Eligible Institutions and Participating Colleges do not know the identity of a student to whom information is delivered unless and until the student chooses to provide their personal information directly to the Eligible Institution or Participating College, which the student can only do outside of the App and outside of the Educational Services. A student may be able to link from the App, email, or QR code in a mailing to further content within BigFuture School or to an external webpage or webform hosted by that Eligible Institution or Participating College. Any preliminary offer of admission will include a school-specific website link through which the student may share their information directly with the Participating College, after which the Participating College may inform the student about any next steps to enroll as well as to be considered for any financial aid. 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 or Participating Colleges other than in de-identified and aggregated form.

Content provided to students through Connections is created by Eligible Institutions and Participating Colleges and may include text, images, videos, and interactive elements. While Connections may be personalized by College Board (e.g., student name at the top of an email) through automated means, College Board is not responsible for and does not create, edit, or approve of the Content. Notwithstanding the foregoing, College Board may send a communication to the student alerting them that information through Connections is forthcoming and/or available in BigFuture School for them to access.



For students who receive a preliminary offer of admission, there is no guarantee of admission, scholarships, or financial aid and it may require them to complete additional steps to accept the offer as defined by the Participating College(s). The Participating College(s) may also require confirmation of information it relied upon in making a preliminary offer of admission, such as requiring the student to submit their final transcript to complete the admissions process. Each Participating College makes the decision on preliminary offers of admission. College Board is not involved in any of the selection or decision making by the Participating College(s).

*\*Not offered in New York at this time. There may be other exclusions.*

#### ADDITIONAL DETAILS REGARDING EDUCATIONAL SERVICES:

*There is no incremental cost for Educational Services.*

*College Board shall provide Client 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, Use, and Disclosure of Data" section. College Board also uses that information in Educational Services, as described above, and to communicate with students about their Covered Assessment(s) and the Educational Services. For students who use the Educational Services, they may be able to update this information within the Educational Services, if they so choose. **All questions are optional.***

*Questions include the following:*

- Home/Mailing Address*
- 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 (for students testing outside the United States)

*To use the App, College Board will provide a secure method for the student to access and authenticate their identity using information collected about them in connection with the Covered Assessment(s) and Educational Services. This may include Client providing student information for this purpose, including, for example, student email address, students providing a mobile number during the administration of the Covered Assessment with their phone number then being used to authenticate into the App, and/or Client providing an access code to each student. By providing their mobile number, the student authorizes College Board to text them to download the App, authenticate into the App, and about their scores, including when their scores are available for Covered Assessments. College Board does not use mobile numbers collected during Covered Assessments for any other purposes. Students are encouraged to provide an email address solely for App account recovery purposes. The foregoing is clearly explained to the student.*

*Client may direct College Board to automatically exclude its students from Connections for the Covered Assessment(s) under this Agreement by contacting College Board Customer Service at (866) 609-1369. Client may visit [collegeboard.org/connections-tc](http://collegeboard.org/connections-tc) for more information about Connections and for access to an opt-out form.*

- *Opt-outs must be submitted before the a deadline communicated by College Board in order to suppress displaying the Connections opt-in to students during their testing experience for the Covered Assessment(s).*
- *If a student had already opted-in to Connections under this Agreement before Client opted-out, the student's data from Covered Assessment(s) under this Agreement will no longer be used for Connections upon College Board's implementation of Client's opt out*
- *If Client excludes its students from Connections and a student is not participating in Connections through other assessment(s) outside of this Agreement, the student will not receive any new content or messaging, and anything previously delivered may be still accessed by student.*

*- If Client opts-out, scores the student received on Covered Assessment(s) may still be used for*



Connections as described above if the student opted-in to Connections through an agreement between College Board and their school, district, or state which has access to Covered Assessment score(s).

- In some instances, Client's state may have elected to opt-out its students and College Board will abide by that exclusion for Client's students.
- If Client opts-out, Client 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](mailto:sateducator@collegeboard.org).
- Upon opt-out, students will still be able to use BigFuture School to receive Score Information and Recommendations.

Students may have opportunities to link from BigFuture School to BigFuture® and to other college and career planning services on College Board's website, [www.collegeboard.org](http://www.collegeboard.org). Those services are not part of Educational Services and do not use student data collected under the Covered Assessments which are the subject matter of this Agreement or any DPA; the only exception being scores on College Board assessments, as all students have independent rights in their own test scores, as further acknowledged above. 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 in the Educational Services. 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](http://collegeboard.org/privacycenter).