DocuSign Envelope ID: 78A04D5B-E476-48EF-8BAD-F088F131542B

DISTRICT OPT-IN AGREEMENT
TO COLLEGE BOARD DATA PRIVACY AGREEMENT

WHEREAS, College Board having its offices at 250 Vesey Street, New York, NY 10281 and the Albany-Schoharie-Schenectady-Saratoga Board of Cooperative Educational Services, having its offices at 900 Watervliet-Shaker Road, Albany, New York 12205 (hereinafter "BOCES"), are parties to a data privacy agreement executed on September 18, 2023 (hereinafter the "DPA"); and,

WHEREAS, such DPA was enacted for the purpose of ensuring the contractual arrangement between College Board and BOCES conforms to the requirements of New York Education Law § 2-d and Part 121 of the regulations of the Commissioner of Education; and

WHEREAS, Jamestown City School District pursuant to Art. IV(3) of the DPA, wishes to acknowledge the terms of the DPA and affirm that the student data and/or teacher or principal data College Board may have access to is subject to its terms.

NOW THEREFORE, District attests and agrees as follows:

1. Jamestown City School District has reviewed the terms of the College Board DPA.
2. Jamestown City School District hereby "opts-in" to the DPA. Jamestown City School District further agrees and acknowledges that student data and/or teacher or principal data to which College Board has access to pursuant to a contract between College Board and Jamestown City School District is subject to the terms of that DPA.
3. Receipt of this document by BOCES and College Board constitutes notice of decision to opt-in to the DPA.

AGREED TO BY:

ORGANIZATION: Jamestown City School District

SIGNATURE: DocuSigned by: Jessie Joy FE378BCC3DAD4E7...

NAME: Jessie Joy

TITLE: Executive Director of Information & Student Services

DATE: 9/22/2023

AGREED TO BY:

ORGANIZATION: College Board

SIGNATURE: DocuSigned by: Jeremy Singer F82EBB4861DE49A...

NAME: Jeremy Singer

TITLE: President

DATE: 9/22/2023

DocuSign Envelope ID: 043C1E41-30AF-4A87-B228-F7DCC13DF46A

CAPITAL REGION BOCES
Approved: 9-18-23

DATA PRIVACY AGREEMENT

Albany-Schoharie-Schenectady-Saratoga BOCES

and

College Board

This Data Privacy Agreement ("DPA") is by and between the Albany-Schoharie-Schenectady-Saratoga BOCES("EA"), an Educational Agency, and College Board ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below. For purposes of this Agreement, PII refers to PII provided pursuant to a contract between College Board and the Education Agency.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**
   In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract effective when signed by both parties for the provision of Contractor's SAT® Suite of Assessments ("Service Agreement"); Contractor may receive PII regulated to the extent applicable by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**
Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate applicable New York laws referenced in Article II Section 1 above.

3. **Data Security and Privacy Plan.**
Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with applicable New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d, to the extent applicable for the Services provided under the Service Agreement, requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C for the sake of convenience and solely to the extent Education Law Section 2-d may apply.

4. **EA's Data Security and Privacy Policy**
State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies to the extent applicable for the Services provided under the Service Agreement.

5. **Right of Review and Audit.**
Upon request by the EA, Contractor shall provide the EA with a copy of its SOC II type report, which Contractor maintains and will continue to maintain during the term of the Service Agreement. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. **Contractor's Employees and Subcontractors.**
   (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall

be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

(b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Contractor must not disclose PII to any other party except as set forth in the Service Agreement and as described herein on Attachment 1, attached hereto and incorporated herein by this reference, unless:

(i) The Contractor has received written permission from a parent or eligible student to whom the data pertains to beforehand; or

(ii) Such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued

access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose in violation of Education Law 2-d, to the extent applicable for the Services provided under the Service Agreement.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d to the extent applicable for the Services provided under the Service Agreement. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Name: KellyRose Yaeger, Esq.

Title: Data Protection Officer

Address: 900 Watervliet-Shaker Road

City, State, Zip: Albany, New York 12205

Email: dpo@neric.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

3. School District or BOCES Opt-in

Any school district or BOCES within New York State may bind itself and Contractor to the terms of this DPA by opting into the terms of this DPA by informing the Parties of its desire to do so in writing on a form prepared by EA. Contractor's recourse in the event of a breach of this DPA by any school district or BOCES shall be limited to recourse against the breaching school district or BOCES and shall not extend to any other school district or BOCES.

EDUCATIONAL AGENCY	CONTRACTOR
Signature:	Signature: DocuSigned by: Jeremy Singer BE2EF27F2DE045D...
Name: JOHN PHELAN	Name: Jeremy Singer
Title: BOARD PRESIDENT	Title: President
Date: 9-18-23	Date: 08/31/2023

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

PARENT BILL OF RIGHTS

Albany-Schoharie-Schenectady-Saratoga BOCES (Capital Region BOCES), in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov/data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, (518) 464-5139, DPO@neric.org, Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that BOCES engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, (518)-464-5139, DPO@neric.org, 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on BOCES' website https://www.capitalregionboces.org/.

CONTRACTOR	
[Signature] X	DocuSigned by: Jeremy Singer BE2EF27F2DE045D...
[Printed Name] JOHN PHELAN	Jeremy Singer
[Title] BOARD PRESIDENT	President
Date: 9-18-23	08/31/2023

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

TO THE EXTENT APPLICABLE FOR THE SERVICES UNDER THE SERVICE AGREEMENT

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	**College Board**
Description of the purpose(s) for which Contractor will receive/access PII	**In connection with College Board's SAT Suite of Assessments, which may include SAT® School Day, PSAT/NMSQT®, PSAT™ 10 and/or PSAT™ 8/9.**
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	As Defined in the Service Agreement.
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Contact EA.

Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other:
Encryption	

CONTRACTOR	
[Signature]	DocuSigned by: Jeremy Singer BE2EF27F2DE045D...
[Printed Name] JOHN PHELAN	Jeremy Singer
[Title] BOARD PRESIDENT	President
Date: 9-18-23	08/31/2023

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.** ***TO THE EXTENT APPLICABLE FOR THE SERVICES UNDER THE SERVICE AGREEMENT***

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See Attachment 2
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See Attachment 2
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	See Attachment 2
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	See Attachment 2
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	See Attachment 2
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See Attachment 2
7	Describe your secure destruction practices and how certification will be provided to the EA.	See Attachment 2
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	See Attachment 2
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	See Attachment 2

Attachment 1

LEA/District ("Client") acknowledges and agrees that the data collected from the administration of the assessment ordered under an agreement with Provider ("Vendor" or "College Board") is subject to College Board's privacy policies, available at https://privacy.collegeboard.org.

College Board shall collect from Client, or Participating Schools (as defined in an agreement with College Board to procure the tests), as applicable, the following student data in connection with the registration of the assessments ordered under an agreement with Vendor, 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)
- *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.

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 under the Service Agreement and for the purposes outlined below.

a. For SAT®, State Scholarship Organizations: State affiliated scholarship organizations may receive student data for the purposes of eligibility for a scholarship or recognition program.
b. For SAT, National Presidential Scholars: Eligible students are shared with the US Department of Education for purposes of the U.S. Presidential Scholars Programs.
c. For PSAT™ 10 and PSAT/NMSQT®, 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.
d. 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.
e. Score Reporting to Students.
f. 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.
g. 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).

h. Accommodations: College Board uses student data to process applications for testing accommodations and to communicate with the SSD coordinator and students regarding accommodations.
i. 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.
j. Research: College Board may use de-identified data obtained from student test-takers for psychometric and educational research purposes to evaluate the validity of our assessments and ensure that tests are unbiased in terms of race, gender, and culture. College Board may also use de-identified data to maintain, develop, support, improve and diagnose our services and applications.
k. 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.

Client 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 Agreement related to the collection, maintenance, use, and disclosure of data shall only apply to the data College Board receives in connection with this Agreement. Nothing in this Agreement is intended to diminish or interfere with student rights in their assessment data including student rights to retain and use their test score, and no provisions in this Agreement are intended to address or cover data that College Board has, or may receive, for services which are outside the scope of this Agreement.

College Board agrees to adhere to the Data Protection, Security Measures and Notice provisions below and in Attachment 2.

Data Protection. College Board shall take actions to protect the security and confidentiality of personally identifiable information that may be obtained pursuant to this Agreement in a manner consistent with industry standards. College Board will maintain a SOC 2 Type II 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 pursuant to this Agreement, as determined by College Board. College Board shall host content in a secure environment that uses Web Application Firewalls/security groups and other advanced technologies designed to prevent interference or access from outside intruders.

College Board encrypts personally identifiable information that may be obtained pursuant to this Agreement in transmission and storage. When College Board's platforms are accessed using a supported web browser, Transport Layer Security ("TLS") 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.

Client 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 Agreement by contract to subcontractors used by College Board, if any, to provide services related to this Agreement. College Board will use appropriate and reliable storage media, regularly backup data and retain such backup copies for the duration of this Agreement, as defined by College Board. Client 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 this Agreement in the United States.

Big Future Mobile App (available for **PSAT/NMSQT Schedule (Fall), PSAT 10 Schedule (Spring), SAT School Day Schedule (Spring))**

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 this Agreement and pursuant to other agreements that College Board has with a client'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.

ADDITIONAL DETAILS REGARDING EDUCATIONAL SERVICES:

There is no incremental cost for Educational Services.

College Board shall provide Client with reporting on your 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.

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, information 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.

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 this Agreement, 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. More information about College Board's Privacy Policies is located at collegeboard.org/privacycenter.

Attachment 2

DATA PROTECTION, SECURITY MEASURES AND NOTICE

College Board shall take actions to ensure the security and confidentiality of security and confidentiality of personally identifiable information that may be obtained pursuant to this Agreement in a manner consistent with industry standards. College Board will maintain a SOC 2 Type II report. College Board assures that personally identifiable data is secured and protected in a manner consistent with industry standards. College Board shall maintain information that may be obtained pursuant to the agreement client has with College Board in a secure computer environment and not copy, reproduce or transmit such data except as necessary to fulfill the purpose of the original request. 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 all stored, managed, retained, accessed or used personally identifiable information that may be obtained pursuant to this Agreement, as determined by College Board. College Board shall host content in a secure environment that uses Web Application Firewalls/security groups and other advanced technologies designed to prevent interference or access from outside intruders.

College Board encrypts personally identifiable information that may be obtained pursuant to this Agreement 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, Transport Layer Security ("TLS") 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.

College Board may use de-identified data: to improve its program, to demonstrate the effectiveness of its program, and for research or other purposes related to developing and improving its program. College Board's use of such de-ientified data will survive termination of any agreement client has with College Board. 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.

Customers 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.

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 use the products and services, if any.

To ensure the security and confidentiality of confidential records College Board shall designate an employee responsible for the training and compliance of all College Board employees, agents, and assigns on compliance with security and confidentiality provisions detailed in the agreement College Board has with client. College Board shall not disclose student records, except as specified under the terms of the agreement College Board has with client, an amendment or as required by law. College Board will extend the confidentiality requirements and security measures identified in this Agreement by contract to subcontractors used by College Board, if any, to provide services related to this Agreement. College Board will use appropriate and reliable storage media, regularly backup data and retain such backup copies for the duration of this Agreement, as defined by College Board. LEA/District 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 this Agreement in the United States.

Our information security policies have received upper management's commitment, support, and direction for managing risks to personal information and their respective systems. Access to personal information is only granted to personnel who have been authorized to handle such type of information and on a need-to-know basis. College Board practices security defense in depth, including forward leaning threat hunting practices. At College Board, information security is everyone's responsibility, and we train and educate our personnel regarding their critical role and responsibilities in protecting all personal information.

LEA/District acknowledges that students may desire to continue and further develop a direct relationship beyond the use of the products which are being provided to students in connection with this Agreement 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 Agreement related to the collection, maintenance, use, and disclosure of data shall only apply to the data College Board receives in connection with the services which are the subject matter of this Agreement. No provisions in this Agreement are intended to address or cover data that College Board has, or may receive, for services which are outside the scope of this Agreement.

College Board offers this as our Data Privacy and Security Plan along with our SOC 2 Type II report.