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

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).

TO THE EXTENT APPLICABLE FOR THE SERVICES UNDER THE SERVICE AGREEMENT

Name of Contractor	College Board
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher ID b. Name c. Birthdate d. Gender e. Race f. Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT. If you collect the PII information above, please complete the remainder of this form.
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: ☐ x Student PII ☐ APPR PII

Contract Term	Contract Start Date 7/1/23 Contract End Date 6/30/24 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. ☒ x 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	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
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) ☒ X Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Please see Attachment 2.
Encryption	Data will be encrypted while in motion and at rest.

Page Left Blank Intentionally

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	See Attachment 2.

Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, 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); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: dpo@wsboces.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	DocuSigned by: Jeremy Singer BE2EF27F2DE045D...
[Printed Name]	Jeremy Singer
[Title]	President
Date:	09/21/2023

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.