STANDARD STUDENT DATA PRIVACY AGREEMENT

(NDPA Standard Version 1.0/ with Exhibit E)

Scottsdale Unified School District #48

and

College Board
(SAT Suite of Assessments)

Version: 1r6

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: Scottsdale Unified School District #48, 8500 E. Jackrabbit Rd., Scottsdale, AZ 85251(the "**Local Education Agency**" or "**LEA**") and College Board, 250 Vesey Street, New York, NY 10281

(the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA for the SAT Suite of Assessments.

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 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

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:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***
   - □ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
   - □ X If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**
   - □ If checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three (3) years. **Exhibit "E"** will expire three (3) years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Scott Menzel Title: Superintendent

Address: 8500 E Jackrabbit Rd., Scottsdale, AZ 85250

Phone: 480-484-6100 Email: smenzel@susd.org

The designated representative for the Provider for this DPA is:

Name: Lee McIllroy Title: Director, K12

Address: 250 Vesey Street, New York, NY 10281

Phone: 480-620-7038 Email: lmcilroy@collegeboard.org

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

LEA

By: Scott A Menzel Date: 5/29/24 08:21 MST

Printed Name: Scott Menzel Title/Position: Superintendent

By: Date: 5/17/24 05:50 MST

Printed Name: Jeremy Singer Title/Position: President

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local 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. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C".** In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) 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 or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact 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, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors**. Provider shall enter into written agreements 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.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
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. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents 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 or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of 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 other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development 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 Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.

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. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. 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 teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the mutually agreed upon third party provider contracted by LEA at their expense to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
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. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions: Jason Ehlert, Vice President, Information Security/CISO; jason@geniussis.com.
4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
    (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
        i. The name and contact information of the reporting LEA subject to this section.
        ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
        iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

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

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **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. 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, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service 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. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **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.

6. **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.

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. 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. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority**. Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder 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"

DESCRIPTION OF SERVICES

Digital SAT® Suite of Assessments including: PSAT™ 8/9, PSAT™ 10, PSAT/NMSQT®[1] and SAT® School Day.

DIGITAL SAT® SUITE OF ASSESSMENT TESTING USING BLUEBOOK
Data Privacy and Security Information

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)
- *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.

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

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

- For SAT, State Scholarship Organizations: State affiliated scholarship organizations may receive student data for the purposes of eligibility for a scholarship or recognition program.
- For SAT, National Presidential Scholars: Data about eligible students are shared with the US Department of Education for purposes of the U.S. Presidential Scholars Programs.
- For PSAT/NMSQT and PSAT10, National Recognition Programs: College Board uses student data to determine eligibility and administer its National Recognition Programs and share information with the 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 in accordance with the PSAT/NMSQT Student Guide and www.nationalmerit.org.
- 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 and to communicate with the SSD coordinator and students regarding accommodations.
- Test Security: College Board may use student data to identify and investigate potential test security incidents, communicate with students about any such incidents, and protect and enhance test security. College Board may disclose the results of test security investigations with third parties, including to the student's school, any score recipient, college, higher education institution or agency, scholarship organization, potential score recipient, government agency in the U.S or abroad, parents, legal guardians, or law enforcement.
- Research: College Board may use de-identified data obtained from student test-takers for psychometric and educational research purposes to evaluate the validity of College Board assessments and ensure that tests are unbiased in terms of race, gender, and culture. College may use de-identified data to demonstrate the effectiveness of College Board programs and services. College Board may also use data to maintain, develop, support, improve and diagnose our services and applications.
- Operational Third Parties: College Board may use and disclose personally identifiable information to third parties providing services to College Board as necessary for its performance of the services in this Agreement and others necessary to administer the SAT Suite and related services. These vendors cannot relicense, sell, rent, or otherwise repurpose the information. These organizations have contractual requirements to protect personally identifiable information from unauthorized access, use, or disclosure.
- 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.

College Board may retain information as needed for legitimate educational purposes, to provide services to students or their educational institution, comply with legal obligations, resolve disputes, and enforce College Board's agreements, which survive expiration of this Agreement.

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 any separate data privacy addendum or agreement ("DPA") related to the collection, maintenance, use, and disclosure of data shall only apply to the data College Board receives in connection with the SAT Suite of Assessments which are subject to any such DPA. Nothing in this Agreement or any DPA is intended to diminish or interfere with student's personal rights in their assessment data, as students have rights independent of this Agreement to access, retain and use their test scores, including from Covered Assessments, and no provisions in any DPA are intended to address or cover data that College Board has, or may receive, for services which are outside the scope of any DPA or agreement with College Board.

College Board Data Protection and Security Measures

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 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.

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 where technically feasible and reasonable, as determined solely by College Board.

College Board's College and Career Readiness Educational Services

With the Covered Assessments, 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, BigFuture® School, that students age 13 and older can download from the App Store to access Educational Services. The App is only available for students taking the SAT School Day,

PSAT/NMSQT and PSAT 10. "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.

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 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 a College Board program through which students are provided information about non-profit colleges, universities, scholarship organizations and other nonprofit educational organizations ("Eligible Institutions") based on criteria provided by those Eligible Institutions, which may include student interests, demographics, students' use of Educational Services, and other information collected by College Board during Covered Assessment(s) for which the student opts-in to Connections (collectively, "Messages"). The 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) may also influence and personalize the students' experiences within BigFuture School and the content of Messages. For Messages from Eligible Institutions, assessment score ranges the student received on past and future SAT, AP, PSAT/NMSQT and PSAT10 assessments may be used. **College Board never shares students' personally identifiable information with Eligible Institutions 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. Students can opt-out any time, as described more fully below.

Opted-in students may receive Messages from Eligible Institutions 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 downloads the mobile application, all of which data elements are optional. Eligible Institutions do not know the identity of a student to whom Messages are delivered unless and until the student chooses to provide their personal information directly to the Eligible Institution, which the student can only do outside of the App and outside of the Educational Services. 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. College Board may track students' access to such links/webpages for purposes of reporting and analytics, but College Board will not disclose such information to Eligible Institutions other than in de-identified and aggregated form.

Messages are created by Eligible Institutions and may include text, images, videos, and interactive elements. While the Messages may be personalized by College Board (e.g., student name at the top of an email) through automated

means, College Board does not create, edit, or approve of Messages and is not responsible for Messages. Notwithstanding the foregoing, College Board may send a communication to the student alerting them that Message(s) are forthcoming and/or available in BigFuture School for them to access.

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

*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 students providing a mobile number during the administration of the Covered Assessment with their phone number then being used to authenticate into the App. Students 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, 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. The foregoing is clearly explained to the student.

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

- Opt-outs must be submitted before the a deadline communicated by College Board for each assessment 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 before Client opted-out of Connections for a Covered Assessment, (i) the student's data from Covered Assessment(s) for which Client opted out of Connections will no longer be used for Connections upon College Board's implementation of Client's opt out; (ii) the student's data from any Covered Assessment(s) for which Client chose not to opt-out of Connections may continue to be used for Connections and the student may still use the Connections feature within the App; and (iii) if Client excludes its students from Connections for all Covered Assessments, use of the student data for Connections for those Covered Assessments will cease upon College Board's implementation of Client's opt out, the students will not receive any new Messages, and any previously delivered Messages may be still accessed by students.
- 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.
- If Client opts-out, Client's students will not going forward be able to opt-in to Connections for the Covered Assessment(s) for which Client opted out of Connections.
- 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. 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.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	x
	Place of Birth	
	Gender	x
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X AI Code
	Student grade level	x
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	

Category of Data	Elements	Check if Used by Your System
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	Optional x
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	x
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	Test Administration Indicator (Which assessment) Season for Testing (Fall, Spring)
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"

DEFINITIONS

De-Identified Data and De-Identification: 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 individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

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.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

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

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.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. 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 constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

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 Student Data.

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

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 operator's 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 any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[Insert categories of data here]

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

2. Nature of Disposition

_____Disposition shall be by destruction or deletion of data.

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

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____As soon as commercially practicable.

_____By [_____]Date

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Provider Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between Scottsdale Unified School District ("Originating LEA") dated 5/17/24 05:50 MST, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:contractsmanagement@collegeboard.org_

BY: _____ Date: 5/17/24 05:50 MST

Printed Name: Jeremy Singer Title/Position: President

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Scottsdale Unified School District and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

[_____Subscribing LEA]

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____ Title: _____

Address: _____

Telephone Number: _____ Email: _____

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
x	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "H"

Additional Terms or Modifications

Version _____

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

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

618-1/4715859.1

PROVIDER:

MODIFICATION TO ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS, Section 3 is hereby amended to add the following language:

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
Provider may transfer pupil-generated content to a separate account where not unduly burdensome and make reasonable efforts to do so, according to the procedures set forth below. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Modification to Article IV: Duties of Provider, Article IV: Section 3 is hereby amended to add the following language:

1. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents 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 or agent with access to Student Data pursuant to the Service Agreement or require such employees and agents to agree to be bound by confidentiality provisions that are equally as restrictive as those set forth in this DPA.

MODIFICATION TO ARTICLE V: DATA PROVISIONS, Article V: Section 2 is hereby amended to add the following language:

2. **Audits.** Upon a written request of the LEA, the Provider will provide a copy of an independent third-party audit conducted based on ISO27001/SOC2.. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the mutually agreed upon third party provider contracted by LEA at their expense to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and anystate, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

Modification to Article V, Section 4 Data Breach, Article V, section 4 is hereby amended to add the following language:

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

MODIFICATION TO ARTICLE VII: MISCELLANEOUS, Article VII: Section 4 is hereby amended to add the following language:

4. **Entire Agreement**. This DPA and the Service 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 with respect to the assessments which are the subject matter of this DPA. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

Modification to Article VII of the DPA, Article VII is hereby amended to include the following language:

10. Select Termination of Access. The LEA may at its sole discretion disqualify at any time any person, entity or Subprocessor authorized to access the LEA's Data by or pursuant to this DPA. Notice of disqualification shall be in writing and shall terminate a disqualified person's or entity's access to any information provided by the LEA pursuant to this DPA immediately upon delivery of the notice to the office of the Provider. Disqualification of one or more persons or entities by the LEA does not affect other persons or entities authorized by or pursuant to this DPA.

Modification to Exhibit C of the DPA, Exhibit C is hereby amended to add the following definitions:

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

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

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

LEA: Scottsdale Unified School District #48

By signing this agreement, the vendor recognizes all standards for the collection and management of data extends to all educators, staff members and parent/guardians of students within the educational organization.