STUDENT DATA SHARING AGREEMENT

Prometric and the Educational Institution are committed to protect personally identifiable student information and other regulated data exchanged between them as required by US Federal Laws and other applicable laws and regulations, and they desire to enter into the DSA for the purpose of establishing their respective obligations and duties.

Article I: Purpose and scope

1. Purpose of the DSA

Prometric and the Educational Institution agree that the purpose of the DSA is to detail the obligations of both Parties relative to the safety and confidentiality of student information, student records and student-generated content (collectively, "Student Data"), which Student Data may be provided to the Provider in connection with the Provider's provision service.

The purpose of the DSA is to establish a comprehensive framework that governs the collection, use, transmission, storage, destruction and protection of Student Data within the K-12 educational environment.

The purpose of the DSA is to provide transparency for various stakeholders including, but not limited to, families, educators, administrators, and local school board members. By adhering to the principles outlined in the DSA, both parties aim to foster an educational environment where the privacy of students is respected, and their Student Data is used responsibly to enhance their educational experience while minimizing risks to their personal and emotional well-being. The commitment to the DSA serves not only to comply with legal requirements but also to uphold the fundamental right of every child to a safe and supportive learning environment, free from intrusive data practices or exploitation.

2. Definitions

"De-Identified Data": Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific 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. Typically, a computer system will store a student's name, student ID number, birthdate, etc. along with their attendance data, assessment scores, and/or usage of a software program. In that situation, a researcher or other party knows exactly which data goes with which student, and the students are "identifiable." De-identified Data, on the other hand, is data where student names, student ID numbers, dates of birth, etc. have all been removed such that no one knows who the students are when analyzing the data. According to the U.S. Department of Education, "*De-identified data may be shared without the consent required by FERPA*[1]*with any party for any purpose, including parents, general public, and researchers*.[2]"

[1] 34 CFR §99.30
[2] 34 CFR §99.31(b)(1)

"Federal Laws": Several relevant federal statutes and their implementing regulations including, but not limited to, the Family Educational Rights and Privacy Act ("FERPA"[3]), the Children's Online Protection Act ("COPPA"[4]), and Protection of Pupil Rights Amendment ("PPRA"[5]).

"Privacy Measures": When publishing tables, cell suppression and other methods of disclosure avoidance can be used to ensure students cannot be identified through small numbers displayed in table cells. The Provider must mask any cells containing fewer than five students and may be required to mask further to avoid any risk that data could be paired with other available data to identify students. The Provider agrees to mask data in such a way to avoid this risk.

"*Provider*": is Prometric.

"Security Measures": the Provider shall develop and implement procedures, and systems to ensure that all Student Data and staff data processed, stored, and/or transmitted under the provisions of the DSA shall be maintained in a secure manner that prevents the interception, diversion, or other unauthorized access to said data. The procedures and systems developed and implemented to process, store, or transmit data provided under the DSA shall be designed to ensure that any and all disclosures of Student Data and staff data comply with all provisions of Federal laws and state laws relating to the privacy rights of students and staff as such laws are applicable to the parties to the DSA. The Security Measures can be found in Exhibit 2 of the DSA.

"School Official": For the purposes of the DSA[6], 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 signed between the Parties.

"Student": Minors enrolled in K-12 education. Kindergarten (K) for 5–6-year-old through twelfth grade (12) for 17–18-year-olds.

"Student Data": Student Data includes any data, whether gathered by Provider or provided by the Educational Institution 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, political affiliations, religious information, 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. Other personal data may be added to this definition in Exhibit 1.

"Subprocessor": means a party other than the Educational Institution or Provider, who Provider uses for data collection, analytics, storage, or other service to operate or improve its service, and who has access to Student Data.

[3] 20 U.S.C. § 1232g (34 CFR Part 99)
[4] 15 U.S.C. § 6501-6506 (16 CFR Part 312)
[5] at 20 U.S.C. 1232h (34 CFR Part 98)
[6] Pursuant to 34 CFR § 99.31(b)

For the purpose of the DSA, the definition of "education records" is set out in 34 C.F.R. § 99.3.

3. Details of Student Data submission

The Student Data provided shall only include information directly relevant to the services agreed upon, and shall exclude any personally identifiable information that is not necessary for the fulfilment of the Provider's obligations. The Provider shall provide the Educational Institution with a detailed list of the specific types of student data that will be collected, which may include in the DSA and other relevant Student Data as agreed upon by both parties.

Article II: Data control and access rights

1. Access rights of legal guardians

The Educational Institution shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review 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 to the Educational Institution'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 Educational Institution.

Before data collection, a clear and detailed notice must be sent to parents, explaining the types of information collected, the methods of collection, the intended uses of the data, and the option to opt out of this collection.

2. Educational Institution's Student Data

All Student Data transmitted to the Provider pursuant to a Service Agreement is and will continue to be under the control of the Educational Institution. Except as expressly set out in the DSA, the Provider does not own any Student Data. The Educational Institution 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 the DSA in the same manner as the original Student Data. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the Educational Institution as it pertains to the use of Student Data.

3. Requests from law enforcement authorities

In the event that law enforcement or any other governmental agency contacts the Provider with a request for Student Data that the Provider holds pursuant to the Services, the Provider shall make all reasonable efforts to notify the Educational Institution prior to any disclosure required by law to the requesting party. This notification requirement shall not apply if the Provider is legally prohibited by the requesting entity from informing the Educational Institution of such a request.

Article III: Duties of the Educational Institution

1. Annual disclosure of student and parent rights

If the Educational Institution has a policy of disclosing Student Data under FERPA[7], the Educational Institution 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.

[7] 34 CFR § 99.31(a)(1)

2. Implementation of adequate safeguards

The Educational Institution shall implement reasonable Security Measures to protect usernames, passwords, and any other credentials that grant access to the services and the Student Data hosted therein.

3. Unauthorized access notification
The Educational Institution shall promptly inform the Provider of any detected instances of unauthorized access to Student Data. Furthermore, the Educational Institution agrees to actively support the Provider in its efforts to investigate and respond to any such unauthorized access incidents.

Article IV: Duties of the Provider

1. Permitted uses of Student Data

The Student Data disclosed in accordance with the Service Agreement shall be strictly utilized solely for the purposes outlined in the Service Agreement or as otherwise expressly authorized by the applicable statutes referenced within the DSA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning; or to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in the DSA.

2. Prohibition on unauthorized disclosure

The Provider acknowledges and agrees that it shall not re-disclose any Student Data or any portion thereof, including but not limited to user content or other non-public information and/or personally identifiable information contained within the Student Data, except as expressly authorized by the Educational Institution or as permitted by the provisions of the DSA. This restriction on disclosure does not apply to aggregate summaries of De-Identified information, which may be used or shared in accordance with applicable data privacy standards.

3. Provider employee obligation

The Provider shall ensure that all of its employees and agents who have access to Student Data strictly adhere to the provisions of the DSA concerning the handling of Student Data as outlined in the Service Agreement. The Provider further commits to obtaining and maintaining a binding confidentiality agreement from each employee or agent with access to Student Data, ensuring their compliance with the terms of the Service Agreement and the obligations specified within the DSA.

4. Compliance with privacy regulations

The Provider should display an easily accessible privacy policy that transparently details the practices for collecting, using, and sharing Student data. This policy must be understandable to legal guardian and clearly visible on the website or digital platform.

5. De-Identified Data

The Provider agrees not to engage in any attempts to re-identify De-Identified Student Data. Such data may be utilized by the Provider for purposes allowed under FERPA, including: (1) supporting the Educational Institution or governmental agencies in research and studies; (2) conducting research and development of the Provider's educational products, and demonstrating the effectiveness of its services; and (3) enabling adaptive learning and personalized student instruction.

The Educational Institution retains an express right to review any data prior to publication by the Provider and to verify proper disclosure avoidance techniques have been used.

The Provider shall not transfer De-Identified Student Data to any third party, except Subprocessors, unless the Provider agrees in writing not to attempt re-identification, and the Educational Institution provides prior written consent after being duly notified.

6. Data retention and disposal

After receiving a written request from the Educational Institution, the Provider must return, destroy, or obliterate all Student Data obtained under the DSA no later than 60 (sixty) days after the earlier of the end of the term, completion of the Provider's services, or receipt of a written request by the Educational Institution to destroy the same.

This term may be amended only by a written agreement that otherwise complies with 20 U.S.C. § 1232g and its implementing regulations in 34 C.F.R. Part 99. Notwithstanding anything to the contrary, the Provider may, with the written consent of the Educational Institution, retain anonymized Student Data received under the DSA.

Notwithstanding any other term of this or any other agreement, the Educational Institution retains the right to terminate the Provider's access to Student Data without advance notice as necessary to ensure the security of Student Data in compliance with the DSA. Furthermore, an authorized representative of the Educational Institution may, upon ten (10) days written notice, inspect the Provider's security protocols and arrangements to ensure compliance with the DSA.

7. Management of 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 the DSA.

8. Collaboration with the Educational Institution

The Provider agrees to collaborate with the Educational Institution to ensure that an annual notification is distributed to all parents and eligible students. This notification shall include a comprehensive explanation of the rights afforded to parents and students under FERPA, such as the right to access, review, and request amendments to the student's educational records.

Article V: Data management provisions

1. Compliance and security audits

Once a year, or following unauthorized access, upon receipt of a written request from the Educational Institution with at least thirty (30) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the Educational Institution 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 Educational Institution.

2. Standards for data security

Prometric and the Educational Institution agree to protect with reasonable data security procedures any Student Data it receives or accesses that could make a student's identity traceable. The Provider agrees

to utilize 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. Provider shall follow the technical and organizational Security Measures in *Exhibit 2*. Provider shall provide the contact information of an employee who the Educational Institution may contact if there are any data security concerns or questions.

3. Data storage

Student Data shall be stored within the United States when required by applicable law. Upon request of the Educational Institution, Provider will provide a list of the locations where Student Data is stored.

4. Procedures for handling data breaches

Upon the discovery by the Provider of a breach of security that results in the unauthorized release, disclosure, or acquisition of Student Data, or the suspicion that such a breach may have occurred, the Provider shall provide initial notice to the Educational Institution as soon as possible, within seventy-two (72) hours of confirmation of the incident.
The initial notice shall be delivered to the Educational Institution by electronic mail and shall include the following information, to the extent:

- Date and time of the breach.
- Names of students whose Student Data was released, disclosed or acquired.
- The nature and extent of the breach.
- A list of the types of Student Data that were or are reasonably believed to have been the subject of a breach.

Upon discovery by the Provider of a breach, the Provider shall conduct an investigation and restore the integrity of its data systems after discovery of the breach.

5. Marketing

Parties shall conduct certain surveys, the collection and use of information for marketing purposes, and certain physical exams in accordance with the relevant provisions of the PPRA[8].

Article VI: General provisions

1. Termination of the DSA

In the event that either Party seeks to terminate the DSA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate the DSA and any service agreement or contract without cause upon 15 (fifteen) days written notice. Any duty of confidentiality as to information protected by State and Federal Laws at any time subject to the DSA shall survive the DSA notwithstanding termination of the DSA.

The term of the DSA shall be effective upon execution by both parties and shall terminate when all of the Student Data collected, used, possessed or maintained by the Provider is properly and completely deleted or destroyed or returned to the Educational Institution.

2. Severability clause

Any provision of the DSA 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

[8] at 20 U.S.C. 1232h (34 CFR Part 98

remaining provisions of the DSA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction.

3. Governing Law, venue and jurisdiction

Prometric and the Educational Institution agree that an agreement and any disputes arising from or relating to the DSA, including its formation and validity, shall be governed by the laws of the State of Connecticut. The parties agree that any and all disputes arising from or relating to the DSA, including its formation and validity, shall be settled in the State of Connecticut.

4. Authority

Each party represents that it is authorized to bind to the terms of the DSA, 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 or any portion thereof.

5. Content of the Agreement

The DSA, including and together with any exhibits, attachments, and appendices, must constitute the entire agreement between the Parties with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, regarding such subject matter. Nothing in the DSA shall be construed or interpreted to allow either party to maintain, use, disclose, or otherwise share Student Data in a manner or not allowed by the state and Federal Laws.

6. Amendment

No amendment to, or modification of the DSA is effective unless it is in writing and signed by Prometric and the Educational Institution. No waiver by any Party of any of the provisions of the DSA shall be effective unless explicitly set forth in writing and signed by the Party so waiving. No failure to exercise, or delay in exercising, any right, remedy, power, or privilege arising from the DSA shall operate or be construed as a waiver thereof, nor shall any single or partial exercise of any right, remedy, power, or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

The DSA is binding on and inures to the benefit of Prometric and the Educational Institution and their respective successors and permitted assignees. Neither Party may assign, transfer, delegate, or subcontract any of its rights or obligations under the DSA without the prior written consent of the other Party. Any purported assignment or delegation in violation of this article shall be null and void. Notwithstanding the foregoing, either party may assign the DSA, without the other party's consent, (i) to any parent, subsidiary, or affiliate entity, or (ii) to any purchase of all or substantially all of such party's assets or to any successor by way of merger, consolidation or similar transaction.

PROMETRIC

Exhibit 1
Student Data used by the Provider

Part 1: Industry-Standard Data

All personal data drafted in Article I section 2, including:

- Student name and student ID
- Teacher name and unique teacher ID
- School name and unique school ID
- Course name and unique course ID
- Student grade level
- Demographic data including gender, date of birth, ethnicity, English proficiency
- status, special education and disability status
- Achievement measures including course grades, national assessment test scores, and state achievement test scores
- Other achievement measures not previously listed which are of interest to stakeholders
- (Approximate) date of administration for each achievement measure provided

PROMETRIC

Exhibit 2

Description of the technical and organizational security measures implemented by the Provider:

- FERPA Security Measures
- National Institute of Standards and Technology (NIST Cybersecurity Framework Version 1.1)
- National Institute of Standards and Technology (NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171)
- International Standards Organization (Information technology — Security techniques
- Information security management systems (ISO 27000 series)
- Center for Internet Security (CIS Critical Security Controls (CSC, CIS Top 20)

1. **Description of technical and organizational security measures**

a. Prometric's Information Security Management System is independently audited and is certified to meet the standards established by the International Standards Organization (ISO) 27000 series of guidance and controls and is assessed to meet or exceed the controls defined in U.S. Government NIST publication 800-53 (with amendments) as well the U.K. Cyber Essentials standard.

b. Prometric requires its vendors through contract to meet one or more of the same standards and confirms compliance through its Vendor Risk Management program.

2. **Pseudonymization and encryption of Personal Data**

a. Prometric encrypts all data in transit and at rest with the industry standard TLS 1.2 and TLS 1.3 configuration and, where appropriate, uses pseudonymizing to protect private data from exposure. This encryption configuration ensures all Prometric data transfers are encrypted with the latest industry standard providing secure communication between web browsers and servers creating a secure connection through symmetric cryptography. Unique keys are generated for each connection based on a TLS handshake negotiated at the beginning of each session. Web browsers utilize an SSL certificate which allows them to recognize that it belongs to a digitally signed certificate authority. Prometric certificates are signed by Digicert who provides SHA-256 cryptographic certificates with RSA-2048 encryption, the industry standard for public-key cryptography against active and passive attacks, which is used in conjunction with 2048 bit keys. Prometric also utilizes a SHA-256 hashing algorithm which protects the integrity of the data and verifies it has not been modified in transit.

b. Prometric requires its vendors to encrypt all sensitive data in transit and at rest and confirms compliance through its Vendor Risk Management program.

3. **Ability to ensure ongoing confidentiality, integrity, availability and resiliency of processing systems and services**

a. Prometric's Information Security Management System is independently audited and/or is certified to meet the standards established by the International Standards Organization (ISO) 27000 series of guidance and controls, is assessed to meet or exceed the controls defined in U.S. Government NIST publication 800-53 (with amendments), is compliant with the Payment Card Industry-Data Security Standards (PCI-DSS), is audited against the SSAE 18 Audit Standards, and is certified to the HMG INFOSEC STANDARD NO. 2. (PCI).

b. Prometric requires its vendors to provide proof at least annually of their continued ability to comply with the foregoing standards and requirements and confirms compliance through its Vendor Risk Management program.

4. **Ability to restore availability and access to Personal Data in a timely manner in the event of physical or technical incident**

a. Prometric's Continuity of Operations Plan and infrastructure are designed in accordance with the guidance of, and Prometric is certified to, ISO 22301, which specifies the requirements for a management system to protect against, reduce the likelihood of and ensure recovery of our business from disruptive incidents.

b. Prometric requires its vendors to have recovery plans and capabilities in place that meet at least minimal industry standards for continuity of operations planning, and confirms compliance through its Vendor Risk Management program.

5. **Process for regularly testing, assessing and evaluating effectiveness of technical and organizational measures for ensuring security of processing**

a. Anti-Virus/Anti-Malware is deployed on all company workstations and servers to prevent, detect and delete viruses and/or malware, such as ransomware, worms or back-doors.

b. Intrusion Protection Systems (IPS) are installed on Prometric networks to detect and prevent attacks, including brute force attacks.

c. Prometric routinely scans systems using automated vulnerability scanners that look for and report potential known vulnerabilities. Prometric also performs annual penetration testing by simulated attacks to assist with finding exploitable vulnerabilities in our environment.

d. Prometric is audited against the SSAE 18 Audit Standard.

c. Prometric requires its vendors to provide annual results from independent security reviews, such as the SSAE 18 Management Letter, and confirms compliance through its Vendor Risk Management program.

6. **The level of security maintained taking into account the risk of accidental or unlawful processing**

a. Prometric employs a multi-layered approach to security with intentional redundancies to increase the security of systems as a whole to address multiple attack vectors while maintaining a high level of security and integrity of data.

b. Prometric's ISMS includes provisions to ensure the confidentiality, integrity and accuracy of all data it processes. All personnel shall annually confirm their adherence to a Code of Business Conduct and Ethics and shall undergo such trainings as to assure their understanding of those expectations. In addition, all personnel shall undergo Security Awareness training and confirm their adherence to Policies that define the need to access only those systems and data types that are required to perform their duties.

b. Prometric requires its vendors to take reasonably effective steps to ensure their personnel are properly screened and receive security awareness and ethics training at least annually and confirms compliance through its Vendor Risk Management program.

The foregoing technical and organisational security measures of the Provider are in place as of the Effective Date of the DSA, but may be subject to change based on future legislation, changing industry standards, or other legal, regulatory or compliance-related reasons. Such changes by Provider shall not be considered a breach of the DSA or the agreement to which it is attached as long as Provider is making such changes to remain in compliance with applicable laws, regulations or industry standards.

Provider's Data Security and Privacy Plan can be accessed at: https://www.prometric.com/privacy-policy.