STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, MISSOURI, NEW HAMPSHIRE, NEW YORK, OHIO, RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA

MA-ME-MO-NH-NY-OH-RI-TN-VT-VA, Modified Version 1.0

BRISTOL WARREN REGIONAL SCHOOL DISTRICT

and

PANORAMA EDUCATION, INC.

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: Bristol Warren Regional School District, located at 151 State Street, Bristol, RI 02809 (the "**Local Education Agency**" or "**LEA**") and Panorama Education, Inc., located at 24 School Street, 4th Floor, Boston, MA 02108 (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

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 **<u>Exhibit "G"</u>** are hereby incorporated by reference into this DPA in their entirety.

   ☑ If Checked, the Provider, has signed **<u>Exhibit "E"</u>** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms 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 years. Exhibit E will expire 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 **<u>Exhibit "A"</u>** (the "**Services**").

6. **<u>Notices</u>**. 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 Provider for this DPA is:

Name: Michael Reynolds Title: Director, Legal

Address: 24 School Street, Fourth Floor, Boston, MA 02108

Phone: 617-356-8123

Email: mreynolds@panoramaed.com

The designated representative for the LEA for this DPA is:

Rose Muller, Technology Director
Bristol Warren Regional School District
151 State Street, Bristol, RI 02809
(401) 253-4000 x5201
Rose.Muller@bwrsd.org

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

BRISTOL WARREN REGIONAL SCHOOL DISTRICT

By: Rosemary O'Connor
Rosemary O'Connor (Sep 30, 2024 12:20 EDT)

Date: 09/30/24

Printed Name: Rosemary O'Connor

Title/Position: Technology Director

PANORAMA EDUCATION, INC.

By: Gayle McGuire

Date: 09 / 26 / 2024

Printed Name: Gayle McGuire

Title/Position: Senior Contract Manager

<u>STANDARD CLAUSES</u>
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **<u>Purpose of DPA</u>**. 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 these 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. **<u>Student Data to Be Provided</u>**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **<u>Exhibit "B"</u>**.

3. **<u>DPA Definitions</u>**. The definition of terms used in this DPA is found in **<u>Exhibit "C"</u>.** 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 and privacy policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **<u>Student Data Property of LEA</u>**. 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. **<u>Parent Access</u>**. 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. **<u>Separate Account</u>**. 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 Data, 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, or a Change of Control. Provider will not sell Student Data to any third party. The provision to not sell Student Data shall not apply to a Change of Control.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data without the written direction of the LEA. De-Identified 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 dispose of Student Data. Except for Subprocessors, Provider agrees not to transfer De-Identified Student Data to any third party unless the transfer is expressly directed or permitted by the LEA or this DPA. 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, unless directed otherwise by the LEA, Provider shall dispose of all Student Data obtained by Provider under the Services Agreement within sixty (60) days of termination (unless otherwise required by law) . 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 Article II, Section 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 a Data Breach, 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 LEA to reasonably 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 facilities, 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. **<u>Data Security</u>**. 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 laws relating to data security and applicable to Provider. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **<u>Exhibit "F"</u>**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **<u>Exhibit "F"</u>**. Provider shall provide, in the Preamble to the DPA, contact information that LEA may use to contact Provider if there are any data security concerns or questions.

4. **<u>Data Breach</u>**. 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 Data Breach response plan that is consistent with applicable industry standards and federal and state law for responding to a Data Breach involving Student Data and agrees to provide LEA, upon reasonable written request, with a summary of said Data Breach 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 Data Breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent reasonably 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 dispose 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 or 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 the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. 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. The LEA has the authority to terminate the DPA within sixty (60) days of receiving notice if the successor does not assume the obligations of this DPA and obligations with respect to Student Data within the Service Agreement, or obligations at least as protective of Student Data as such obligations or entering into business with the successor violates Federal, state or local laws, regulations, or policy.

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

- Panorama Student Success
  - Description:

    Student Success is the market-leading K-12 platform for helping districts translate insights into effective student supports. With unified data and intuitive support planning tools, Student Success makes it easy to understand student needs and provide targeted support to drive academic outcomes. Whatever your district's strategic goals, work to achieve them in Student Success—from improving literacy to increasing attendance to preparing students for college, career, and life.

    Student Success is a one-stop shop that brings together data across academics, attendance, and behavior, offering a holistic view of your district, schools, and students. User-friendly dashboards surface the data you need to proactively identify system-wide and individual student needs. Easily take action to support students with intervention planning workflows, collaboration tools, and hundreds of included strategies. Plus, Panorama's dedicated team of education experts is committed to your success and partners closely with you to meet your district goals and vision.

- Panorama Pathways
  - Description:

    Panorama Pathways is a leading on-time graduation and CTE program tracking solution that ensures your students are ready for college, career, and life. Configured to meet your unique state and district requirements, Pathways automates the complex and manual processes of auditing, reporting, and correcting student transcripts and schedules. Now, worry less about administrative errors that can keep students from graduating on time.

    With student data refreshed daily, Pathways gives you a holistic view of each student's journey to graduation. At-a-glance reports offer powerful insights to help you support students with their transcripts, class schedules, and pathway options. Plus, Panorama's dedicated education experts partner closely with you, offering strategic advising, tailored workshops, and ongoing support to ensure you meet your district's goals and vision.

    Pathways, when combined with our market-leading K–12 MTSS platform, Panorama Student Success, helps district administrators, school leaders, and educators support the whole student across academics, attendance, behavior, life skills, on-time graduation, career readiness, and CTE tracks.

- Panorama Surveys & Engagement
    - Description:
      Panorama Surveys and Engagement is the leading K–12 platform for all your district's survey needs, from benchmark surveys to pulse checks. Panorama is the central place for districts to collect and analyze student, family, and teacher feedback on the factors that are critical to student achievement. With reliable, actionable feedback data, districts can address key issues like belonging, teacher-student relationships, engagement, and school safety.

      Student Surveys offer insight into students’ experiences, mindsets, skills, and perceptions of school climate, safety, and academics. Family Surveys reveal attitudes on important topics and can help boost family engagement. Teacher and Staff Surveys collect data to help district leaders retain educators and improve work and learning environments. The MTSS Implementation Survey gathers input from educators and administrators to enhance MTSS implementation. And the Superintendent First 100 Days Survey helps new superintendents identify priorities during the critical initial phase of their role.

      With research-backed survey instruments, powerful analytics, and expert strategies for taking action, school and district leaders can capture valid and reliable feedback, understand the factors that foster positive learning environments, and take data-driven action to support students. Only Panorama, with our deep K–12 experience and decades of historical data, knows the right questions to ask and how to ask them to track and improve student metrics over time.

- Panorama Check-Ins
    - Description:
      Panorama Check-Ins is a survey tool that empowers educators to quickly and easily gather real-time insights into students’ well-being, learning environment, and immediate needs. Whether you’re a classroom teacher or a district leader, Check-Ins provides valuable information at every level. These insights help you take timely action to support students who may be struggling and measure progress toward long-term district goals.

      With real-time, actionable feedback, you’ll address key challenges across well-being, life skills, and classroom feedback. This instant feedback, combined with our library of proven strategies, gives you the knowledge you need to support your students effectively. Drawing on extensive K–12 experience and deep data insights, Panorama helps you identify the right questions and the most effective ways to ask them, ensuring accurate tracking of student progress.

- Panorama Solara
    - Panorama Solara is a purpose-built AI chat application designed specifically for K-12 districts, prioritizing top security and privacy standards. Solara seamlessly integrates

with your existing Panorama data sources, like Panorama Student Success and Panorama Surveys & Engagement, and aligns with your unique educational practices, helping you support each student’s path to success. It leverages and interacts with your secure student data to make you more efficient throughout your day, whether you need a custom lesson plan or information for targeted student supports.

Educators can trust Solara to provide high-quality content while keeping their data safe, using their district's existing student information to develop strategies like attendance plans. With a library of ready-to-use, research-backed prompts and tools, Solara provides quick access to quality K-12 resources, empowering educators to complete tasks more efficiently, that enables you to spend more time with students and drive learning outcomes. Solara is an essential and secure tool for today’s K-12 districts and schools.

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.	X
	Other application technology meta data-Please specify: See Note 1	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	X
	Observation data	X
	Other assessment data-Please specify: See Note 2	X
Attendance	Student school (daily) attendance data	X
	Student class attendance data	X
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	X
	Other demographic information-Please specify: Any and all demographics are optional. See Note 2	X
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	X
	Specific curriculum programs	X
	Year of graduation	X

Category of Data	Elements	Check if Used by Your System
	Other enrollment information-Please specify: Year entered 9th grade. See Note 2	X
Parent/Guardian Contact Information	Address	X
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts/ health data	
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	X
	Other indicator information-Please specify: Any and all indicators are optional. See Note 2	X
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Provider/App assigned student ID number	X
	Student app username	X
	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)	X

Category of Data	Elements	Check if Used by Your System
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify: Educators have the ability to upload documents to student profiles, which may include student work	X
Transcript	Student course grades	X
	Student course data	X
	Student course grades/ performance scores	X
	Other transcript data - Please specify: See Note 2	X
Transportation	Student bus assignment	X
	Student pick up and/or drop off location	X
	Student bus card ID number	X
	Other transportation data – Please specify: See Note 2	X

Category of Data	Elements	Check if Used by Your System
<u>Other</u>	Please list each additional data element used, stored, or collected by your application: Note 1: operating system, browser version, device type, location (from IP) Note 2: Each LEA determines what data it will make to Provider in connection with the Services, and it may choose to send data not explicitly listed in this Exhibit B, covered by various "Other" categories. Such data is impossible to exhaustively list, because each LEA determines which data is relevant to its work and objectives with Provider. Data that Provider may specifically request or require as part of providing Services is listed in this Exhibit B. Provider expects that each LEA choose a subset of the data in Exhibit B to be used in connection with Provider's Services.	
<u>None</u>	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"
DEFINITIONS

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

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

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 thisDPA.

Originating LEA: An LEA who executes the original 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(a)(1)(i)(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 pursuant to which Provider is performing services for LEA.

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 Metadata that has not been stripped of all direct and indirect identifiers. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Educational 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. Information that has been anonymized or De-Identified Data, or anonymous usage data regarding a student's use of Provider's services shall not constitute Student Data.

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 DPA 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 Educational 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**] 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 [**Insert Date**]

4. Signature

____ ___________________

Authorized Representative of LEA Date

5. Verification of Disposition of Data

____ _______________

Authorized Representative of Company Date

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)**
X	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
X	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)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	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 “G”
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."

2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.

4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.

5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.

6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.

7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:

    a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;

    b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or

    c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT "G"
Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
    a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student's family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include:
        i. Details of the incident, including when it occurred and when it was discovered;
        ii. The type of personal information that was obtained as a result of the breach; and
        iii. The contact person for Provider who has more information about the incident.
    b. "*Breach*" shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
    c. "*Personal information*" is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
        i. Social Security Number;
        ii. Driver's license number or other unique identification number created or collected by a government body;
        iii. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
        iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account;
        v. Medical information; or
        vi. Health insurance information.

EXHIBIT “G”
Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

5. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
6. In Article IV, Section 3, add: “The Provider will restrict unauthorized access by Provider’s employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties.”
7. In Article IV, Section 6, replace “Upon termination of this DPA, unless directed otherwise by the LEA, Provider shall dispose of all Student Data obtained by Provider under the Services Agreement within sixty (60) days of termination (unless otherwise required by law),” with “Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall dispose of or return Student Data to the LEA in accordance with this DPA.”
8. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
9. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
10. Provider will not access or monitor any of the following:

    a. Location-tracking features of a school-issued device;
    b. Audio or visual receiving, transmitting or recording features of a school-issued device;
    c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
    - **i.** Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
        1. The credit reporting agencies
        2. Remediation service providers
        3. The attorney general
    - **ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.
    - **iii.** A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.
    - **iv.** For clarification, the LEA will provide direct notification to affected individuals. Provider will provide LEA contact information to its designated point of contact related to breach (not credit reporting agency or remediation services or an attorney general).

EXHIBIT "G"

Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq.*, T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq.*, T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq.*; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

11. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
12. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
13. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
14. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
15. The Provider agrees that it will not collect individual student data on:
    a. Political affiliation;
    b. Religion;
    c. Voting history; and
    d. Firearms ownership

EXHIBIT "G"
Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT "G"
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

16. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
17. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
18. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
19. In Article V, Section 4, add: In order to ensure the LEA's ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours from when the Provider discovers or confirms Student Data may have been disclosed in a data breach.

EXHIBIT “G”
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to “Student Data” shall be amended to state “Student Data and Teacher Data.” **“**Teacher Data” is defined as at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

“Teacher” means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **<u>Exhibit “I”</u>.**

3. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”

4. In Article IV, Section 7 amend each reference to “students,” to state: “students, teachers,…”

5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use

the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:

(1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;

(2) Limit unsuccessful logon attempts;

(3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;

(4) Authorize wireless access prior to allowing such connections;

(5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

(6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

(7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;

(8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

(9) Enforce a minimum password complexity and change of characters when new passwords are created;

(10)Perform maintenance on organizational systems;

(11)Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;

(12)Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;

(13)Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;

(14)Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

(15)Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;

(16)Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

(17)Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

(18)Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

(19)Protect the confidentiality of Student Data and Teacher Data at rest;

(20)Identify, report, and correct system flaws in a timely manner;

(21)Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22)Monitor system security alerts and advisories and take action in response; and

(23)Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB). For clarification, Provider's security program and documentation is based on ISO-27001/2, however, will be migrating to NIST 800/53 and CyberSecurity Framework. SOC-2 audits are based on this security program.

8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:

   i. The estimated number of students and teachers affected by the breach, if any.

9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify: Operating system browser version, device type, location (from IP)	X
Application Use Statistics	Meta data on user interaction with application	X
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	X
	Other demographic information-Please specify: Staff demographics may be included if staff surveys are administered, although they are optional and inclusion is completely determined by the LEA	X
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	X
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify: Staff indicators may be included if staff surveys are administered, although they are optional and inclusion is completely determined by the LEA	X
Teacher Identifiers	Local (School district) ID number	X
	State ID number	X
	Vendor/App assigned student ID number	X
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	X
Teacher Survey Responses	Teacher responses to surveys or questionnaires	X
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Exhibit "G"

New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.

3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.

4. Provider represents that their Data Privacy and Security Plan is attached as Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a)implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.

5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to "Student Data" shall be amended to include and state, "Student Data and APPR Data."

7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA's Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

8. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."

9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider's employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.

10. To replace Article IV, Section 6 (Disposition of Data) with the following: 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 ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying that it and it's subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider

pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. .

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 ninety (90) days 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",** or, with reasonable notice to the Provider, other form of its choosing. 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".**

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."

12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an 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 LEA or its designee(s) 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 or its designee(s) 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 facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 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; and

    vi. The number of records affected, if known; and

    vii. A description of the investigation undertaken so far; and

    viii. The name of a point of contact for Provider.

    (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. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of legally required notification to Parents, Eligible Students, teachers, and/or principals.

    (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.

(6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Data Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- "Provider" is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure**: The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose

- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District**: As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

Exhibit "J"
LEA Documents

New York LEAs will provide links to their Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement in their Exhibit Es.

<u>Exhibit "K"</u> - Provider Security Policy AND Data Security and Privacy Plan

Provider's Data Security and Privacy Policy can be accessed at https://www.panoramaed.com/privacy

Panorama - DATA PRIVACY AND SECURITY PLAN

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Panorama uses Contract Lifecycle Management (CLM) software to store contracts including any client specific requirements. Panorama is compliant with applicable laws on data privacy, and if there are any client-specific requirements, the contracts team has an internal escalation policy designed specifically for review, approval, and implementation of client requirements. If a client-specific requirement is approved, the requirement is noted in the CLM and implemented thereafter. Further, Panorama's legal team actively reviews state and local laws and informs the contracts team of any necessary updates.
2	Specify the administrative, operational, and technical safeguards and practices that you have in place to protect PII.	See Exhibit C.1. Panorama is fully compliant with the Family Educational Rights and Privacy Act (FERPA), the Pupil Privacy Protection Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), and has signed the Student Privacy Pledge. https://studentprivacypledge.org/ Panorama Education uses Amazon Web Services (AWS) for hosting its systems. AWS is an industry-leading cloud infrastructure services provider for web hosting and data processing. AWS services are continuously and rigorously tested against leading Cybersecurity frameworks, including SOC 2, ISO, HIPAA, and PCI DSS, among others. These assessments are conducted by independent evaluators and their findings are readily available on AWS' website. All Panorama data is hosted and processed in Amazon's us-east-1 region located in Virginia. Further, Panorama uses industry-standard practices for web application architecture, including encryption of data in-transit & at rest, HTTPS communication, and failover databases. Panorama limits its access to cloud systems only to engineers working directly on the platform. All employee access to cloud systems is gated behind single sign-on logins that are unique to each employee and require multi-factor authentication before granting access. When granted, access to cloud systems is ephemeral and expires after a few hours before requiring the employee to log in again. Panorama, in turn, employs teams of engineers dedicated to monitoring platform health and security. Engineering teams use leading cloud security posture tools and security event management systems provided by Amazon, Datadog, and Sentry to detect anomalous activity and protect against intrusions. Panorama maintains an incident response protocol that dictates how incidents are investigated and mitigated. Engineering teams run quarterly drills to test their familiarity with the protocol and to measure their response against incidents related to platform health and security. To validate the strength of Panorama's security posture, Panorama has partnered with Independent Security Evaluators ("ISE") to run penetration tests against platform systems. These tests evaluate the security of Panorama's website and infrastructure systems. On Panorama's website, ISE tests against front-end malicious tactics such as credential stuffing, cross-site scripting, and SQL injection. For platform infrastructure, ISE checks firewall configurations, database security, and internal access controls. Panorama's Security and Privacy programs are guided by publications from the National Institute of Standards and Technology ("NIST") standards. NIST publishes a framework of

		security activities and outcomes that a mature security program is expected to exhibit, including how internal access controls and infrastructure are managed. Panorama internally tracks its programs that are meeting these expectations. Moreover, Panorama has an appointed Trust Council of internal engineering, privacy, security, and legal resources that work alongside the Information Security team to rigorously evaluate, prioritize, and mitigate theoretical risks or gaps. To verify the effectiveness of Panorama's security program, we partner with Schellman & Company, LLC to conduct an annual SOC 2 Type 2 audit to ensure systems are designed and operating effectively to meet trust service criteria related to security and confidentiality. A copy of the most recent SOC 2 Type 2 report or an executive summary of the latest penetration test results is available upon request.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Panorama conducts annual security and privacy training for all employees, during which among other things they are reminded of their obligation to protect PII.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Panorama's agreements with its subcontractors require them to adhere to all applicable laws regarding data privacy and contain terms that are at least as protective of the Educational Agency's data as the ones contained in the Contract. Panorama's legal team and security team review new vendor agreements for consistency.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Panorama maintains an incident response protocol that will be exercised if a data incident is suspected. If Panorama experiences a breach or other incident that triggers the breach notification, Panorama will comply with applicable law(s) and follow the required steps for notification and mitigation. In the case of a reportable breach or equivalent reportable incident, regardless of whether experienced by Panorama or a customer, Panorama will provide the affected customer with information customer may use to respond to inquiries, such as: - What happened - What information was involved - What we are doing about it - What you can do for more information
6	Describe how data will be transitioned to the Educational Agency when no longer needed by you to meet your contractual obligations, if applicable.	Panorama will coordinate with the Educational Agency via the Educational Agency's main point of contact in following the Contract's directions to transition and then subsequently delete the subject data.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Panorama deletes electronic data in accordance with NIST 800-88 r1 at a level of sanitization that makes it impossible to recover data in the normal course of Panorama's data operations and renders it infeasible to recover any data from devices with ordinary techniques. To the extent Panorama identifies print materials in its possession that contain PII, it shreds such materials. Certification will be provided in writing as provided in the Contract.

8	Outline how your data security and privacy program/practices align with the Educational Agency's applicable policies.	Panorama follows the programs and practices that align with NIST's Cybersecurity Framework. See Exhibit C.1.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	Panorama Operations collects information related to all laptop assets. Information documented includes the date the asset was ordered and the make, model, and serial number of the laptops, as well as username for all other devices and systems, reliance is placed on the vendors that support Panorama's IT infrastructure. Panorama maintains a list of applications reviewed for use at Panorama as a related subsection associated with the information security policy. These applications have been reviewed by information Security. Additionally, Panorama maintains a listing of the applications that are approved for use with data classified as Sensitive data. Panorama has deployed a software tool that will limit what software can be installed on Panorama issued laptops and will be able to provide a formal listing of software installed on laptops. Generally, the content of nearly all existing Panorama policies help inform employees of expectations related to organizational communication. As heavy reliance is placed on external vendors to provide infrastructure services that support Panorama services and products, there is good awareness of these vendors and these external information systems have been cataloged.
	Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Panorama has a clear direction in the market and has clearly defined relationships with vendors and customers. Panorama's role is communicated with Panorama employees through the onboarding process and through quarterly goal setting. The majority of critical infrastructure necessary for Panorama is provided by third parties. Documentation exists within Panorama's internal knowledgebase to help Panorama employees understand these relationships. The onboarding process as well as periodic training helps Panorama employees better understand the critical infrastructure.

	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Panorama has documented information security requirements and has made the policy available to Panorama employees within the company knowledgebase. Panorama has a cross-functional "Trust Council" responsible for identifying risks, implementing appropriate protocols, and overseeing the company's privacy and security program. Panorama has documented information security requirements and has made the policy available to Panorama employees within the company knowledgebase. The company's security policies are applicable to all Panorama employees.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Panorama relies on vendors to identify and document asset vulnerabilities in critical infrastructure. Panorama deployed a tool which enforces set security settings on the laptops such as requirements for strong passwords and hard drive encryption. Personal phones used by Panorama employees are also required to have mobile device management software installed which forces the use of a PIN and the use of encryption. Members of Panorama's Trust Council are involved in information sharing forums and receive notifications from vendors related to threat intelligence. Panorama has documented potential business impacts and likelihoods and third-party vendor risks.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Through the existing information security policy content and through onboarding activities, Panorama's risk tolerance is communicated. Critical infrastructure can be determined based on whether it is used to store and process Sensitive data (data that contains student PII and educational records). Further, critical vendors have also been identified and are documented based on the same criteria.

	Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	Panorama vendors are clearly identified and effort is made to review contractual requirements to ensure that adequate availability and data protection requirements are in place. Critical third- party services that are used to store and process Sensitive data have also been identified. Critical third- party vendors are onboarded with highly available services already configured. Where determined necessary, additional resiliency is acquired from these vendors. Close working relationships exist between Panorama team members and the vendors and recovery efforts are jointly made as issues arise.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	All Panorama employees are issued usernames and passwords to access information systems. Credentials are managed, verified, and revoked. Employees are responsible to maintain the physical security of their issued laptops. Requirements for physical security are documented within the information security policy. Employees can log into Panorama information systems remotely. All information systems containing Sensitive data require two factor authentication. Panorama has developed role-based access which limits employees to the access required to perform their job responsibilities. Additionally, the information security policy contains a reference to minimum access necessary to Sensitive data. Reliance on network integrity controls is placed on the vendors (i.e. AWS) that provide infrastructure services. Identities of employees are effectively validated prior to the issuance of credentials.
	Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	All Panorama employees are trained during an onboarding session at the time of hire and then on an annual basis. Information security is one of the areas where training is provided. Privileged employees such as engineers receive additional instruction with role-specific onboarding. Requirements related to third-party stakeholders are formally documented within applicable contracts.

	Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	Panorama requires the encryption of all data at rest. Employees are issued laptops with disk encryption enabled. Employees that utilize their personal mobile phones to conduct business are required to install mobile device management software that forces encryption of data. Vendors providing infrastructure and platform services all encrypt data at rest. Panorama has provided guidance to employees on the appropriate methods for the secure exchange of Sensitive data within the information security policy. Panorama manages laptops throughout the process of purchase, issuance, and retrieval. Assets are stored in a secured area within the office when not in the possession of an employee. All other supporting infrastructure assets are maintained and managed by critical vendors. Panorama maintains close relationships with their critical infrastructure vendors and places reliance on them to monitor for capacity constraints and to notify Panorama if additional resources need to be made available. Panorama has tools in place to generate alerts in data within Google drive when data is made accessible to non-Panorama entities. Reliance is also placed on infrastructure vendors to monitor for data leaks. Integrity checks related to software occur through the SDLC process. Employees are encouraged to download software only from reputable sources. A significant reliance is placed on critical infrastructure service providers to maintain information integrity processes. Panorama utilizes development and staging environments separate from the production environment. All code is tested prior to being deployed in production. Panorama relies on its critical infrastructure service providers to validate hardware integrity and to resolve any issues.

	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Panorama relies on tools provided by its critical infrastructure service providers to monitor baseline configurations and provide notifications related to unusual activity. Panorama follows an Agile process for code development. Peer review and code testing are standard practices and workflows ensure that required steps are followed. Panorama will open Jira tickets for some configuration changes such as the implementation of a new version of software. Tickets are used to document testing and to schedule the change. Panorama relies on its critical infrastructure vendor to perform regular backups of information. Restores of data are common and serve as a test of a backup process. Panorama relies on its critical infrastructure vendor to monitor the physical operating environment and to securely dispose of Panorama data. Additionally, Panorama employees are asked to destroy any Sensitive data that temporarily needs to be stored on the employee's laptop hard drive. The Trust Council meets biweekly and regularly assesses data protection processes. The Trust Council shares the effectiveness of the protection technologies with stakeholders primarily through their participation in the incident management process. Vendors provide highly available platforms and failovers are regular, which also constitute business continuity tests. The incident response process is in place and facilitated by the Trust Council in conjunction with stakeholders. Criminal background checks are performed for all Panorama employees at the time of hire and annually thereafter.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Panorama relies on its critical infrastructure vendors to maintain and repair assets that support Panorama products.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Audit logs are primarily maintained by the critical infrastructure vendors, but Panorama engineers can review logs as necessary to perform their responsibilities. Removable media is rarely used, however if it is required, media will be provided to Panorama employees. Removable media is not approved for storage of Sensitive data. Panorama has implemented the principle of least privilege by assigning roles to employees which only provide them with the access needed to perform their responsibilities. Panorama relies on its critical infrastructure vendors to protect communications and networks and to provide load balancing across its services.

DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	Panorama relies on its critical infrastructure vendors to monitor network baselines and provide notifications for any unusual activities. The Trust Council facilitates the incident management process during which detected events are analyzed and categorized. Panorama relies on its critical infrastructure vendors to maintain audit logs. When the Panorama team is investigating incidents, event data is collected and correlated as necessary to perform their analysis. The Panorama team assesses the impact of the analyzed events, primarily by noting whether Sensitive data was involved.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Panorama relies on its critical infrastructure vendors to monitor the network for security events and to provide notifications to Panorama related to any suspicious activity. Panorama relies on its critical infrastructure vendors to monitor the physical environment for security events and to provide notifications to Panorama related to any suspicious activity. Panorama relies on its critical infrastructure vendors to monitor network baselines and provide notifications for any unusual activities. Panorama relies on its critical infrastructure vendors to monitor for and remediate malicious code. Panorama relies on its critical infrastructure vendors to monitor for and remediate unauthorized mobile code. Panorama relies on its critical infrastructure vendors to perform vulnerability scanning of their environments.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection of events primarily occurs due to processing failures or customer complaints. There are roles and responsibilities associated with the individuals that observe these indicators and reach out to the Trust Council to initiate the incident management process. Panorama relies on its critical infrastructure vendors to provide notifications when unusual activity is found. Panorama performs a root cause analysis for all investigated incidents and works to make improvements to existing processes.

RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	As necessary, response plans are documented and followed to recover from security incidents.

	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Roles related to the incident management process are documented and are assigned to team members at the beginning of the investigation. Detection of events primarily occurs due to processing failures or customer reports. There are roles and responsibilities associated with the individuals that observe these indicators and reach out to the Trust Council to initiate the incident management process. Response plans are developed as the incidents are investigated. If the incident involves Sensitive data, the legal team and the PR team are notified and join the investigation. Information would be shared with customers and other external parties as needed.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Detection of events primarily occurs due to processing failures or customer complaints. There are roles and responsibilities associated with the individuals that observe these indicators and reach out to the Trust Council to initiate the incident management process. Impact associated with the incident is determined primarily on whether Sensitive data was involved. Incidents are categorized primarily by whether Sensitive data was involved. Organization members are trained to understand the critical nature of protecting Sensitive data. The individuals assigned to investigate identified incidents perform basic forensics such as log correlation and analysis. If additional forensics need to be performed, the team will involve experts as necessary. The Trust Council is involved in forums where they can keep updated on new vulnerabilities. Additionally, a close relationship is maintained with critical infrastructure service vendors who also help Panorama become aware of new vulnerabilities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	When the Panorama team is investigating incidents, activities will be coordinated across the team members and/or vendors to contain and mitigate the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Panorama performs a root cause analysis for all investigated incidents and works to make improvements to existing processes.

RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	As necessary, recovery plans are documented and followed to recover from security incidents.

	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Panorama performs a root cause analysis for all investigated incidents and works to make improvements to existing processes.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Panorama has processes in place to communicate with customers in the event of an outage. If a significant breach were to occur, Panorama's executive team members and legal team would ensure proper reporting, communication, and coordination. Panorama's security team would be responsible for repair and restoration activities, including coordinating with critical infrastructure vendors.

Dropbox Sign

Audit trail

Title	TEC 10 State NDPA final 9-24-2024 GeM
File name	TEC 10 State NDPA...9-24-2024 GeM.pdf
Document ID	e6e68d7fa0c06bb514643bdfa13a89d788cf941e
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History

SENT	**09 / 26 / 2024** 16:30:03 UTC	Sent for signature to Gayle McGuire (gmcguire@panoramaed.com) from jchapin@panoramaed.com IP: 73.16.129.254
VIEWED	**09 / 26 / 2024** 16:30:49 UTC	Viewed by Gayle McGuire (gmcguire@panoramaed.com) IP: 73.16.25.0
SIGNED	**09 / 26 / 2024** 16:33:10 UTC	Signed by Gayle McGuire (gmcguire@panoramaed.com) IP: 73.16.25.0
COMPLETED	**09 / 26 / 2024** 16:33:10 UTC	The document has been completed.

Dropbox Sign

Audit trail

Title	TEC 10 State NDPA final 9-24-2024 GeM (1)
File name	TEC 10 State NDPA...-2024 GeM (1).pdf
Document ID	0d945b5a2d4d4a003446f23c7333efa19c068ebd
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History

SENT	**09 / 26 / 2024** 17:24:20 UTC	Sent for signature to Contracts (contracts@panoramaed.com) from jchapin@panoramaed.com IP: 73.16.129.254
VIEWED	**09 / 26 / 2024** 18:18:38 UTC	Viewed by Contracts (contracts@panoramaed.com) IP: 73.16.25.0
SIGNED	**09 / 26 / 2024** 18:21:10 UTC	Signed by Contracts (contracts@panoramaed.com) IP: 73.16.25.0
COMPLETED	**09 / 26 / 2024** 18:21:10 UTC	The document has been completed.

Panorama_BristolWarren_10State_VendorSigned

Final Audit Report 2024-09-30

Created:	2024-09-30
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAzVt2l3bZiFQsIbg--sarueLptU_jdM3x

"Panorama_BristolWarren_10State_VendorSigned" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-09-30 - 4:18:09 PM GMT

Document emailed to rose.oconnor@bwrsd.org for signature
2024-09-30 - 4:18:18 PM GMT

Email viewed by rose.oconnor@bwrsd.org
2024-09-30 - 4:19:50 PM GMT

Signer rose.oconnor@bwrsd.org entered name at signing as Rosemary O'Connor
2024-09-30 - 4:20:46 PM GMT

Document e-signed by Rosemary O'Connor (rose.oconnor@bwrsd.org)
Signature Date: 2024-09-30 - 4:20:48 PM GMT - Time Source: server

Agreement completed.
2024-09-30 - 4:20:48 PM GMT

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: Bristol Warren Regional School District, located at 151 State Street, Bristol, RI 02809 (the "**Local Education Agency**" or "**LEA**") and Panorama Education, Inc., located at 24 School Street, 4th Floor, Boston, MA 02108 (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

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.

   ☑ 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~~,~~ and the Supplemental State ~~or Special Provisions~~Terms, the Supplemental State Terms 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 years. Exhibit E will expire 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.

STANDARD CLAUSES
Version ~~3~~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 these 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~~ and 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~~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.

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~~Data, 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~~.~~, or a Change of Control. Provider will not ~~Sell~~sell Student Data to any third party. The provision to not sell Student Data shall not apply to a Change of Control.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data without the written direction of the LEA. De-Identified 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~~dispose of Student Data. Except for Subprocessors, Provider agrees not to transfer ~~de-identified~~De-Identified Student Data to any third party unless ~~(a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to~~the transfer is expressly directed or permitted by the LEA ~~who has provided prior written consent for such transfer~~or this DPA. 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~~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~~unless directed otherwise by the LEA ~~is received~~, Provider shall dispose of all Student Data ~~after providing~~obtained by Provider under the ~~LEA with reasonable prior notice~~Services Agreement within sixty (60) days of termination (unless otherwise required by law) . 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~~Article II, Section 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~~a Data Breach, 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 LEA to reasonably 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 facilities, 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~~laws relating to data security and applicable to Provider. 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. 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~~Preamble to the DPA, contact information ~~of an employee who~~that LEA may use to contact Provider if there are any data security concerns or questions.

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~~Data Breach response plan that ~~reflects best practices and~~ is consistent with applicable industry standards and federal and state law for responding to a ~~data breach, breach of security, privacy incident or unauthorized acquisition or use of~~Data Breach involving Student Data ~~or any portion thereof, including personally identifiable information~~ and agrees to provide LEA, upon reasonable written request, with a summary of said ~~written incident~~ Data Breach 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~~Data Breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent reasonably 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~~dispose 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 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 the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. 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~~The LEA has the authority to terminate the DPA within sixty (60) days of receiving notice ~~shall include a written, signed assurance that~~ if the successor ~~will~~does not assume the obligations of ~~the~~this 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~~, or obligations at least as protective of Student Data as such obligations or entering into business with the successor ~~to whom the Provider is selling, merging, or otherwise disposing of its business~~violates Federal, state or local laws, regulations, or policy.

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 "C"
DEFINITIONS

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

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

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~~thisDPA.

Originating LEA: An LEA who ~~originally~~ executes the original 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(a)(1)(i)(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~~contract, purchase order or ~~Terms~~terms of ~~Service~~service or ~~Terms~~terms of ~~Use~~use pursuant to which Provider is performing services for LEA.

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~~Metadata that has not been stripped of all direct and indirect identifiers. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute ~~Education~~Educational 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~~Information that has been anonymized or ~~de-identified~~De-Identified Data, or anonymous usage data regarding a student's use of Provider's services shall not constitute Student Data.

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~~DPA 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~~Educational 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 “G”
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

13. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
14. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
15. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
16. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours~~, where~~ from when the Provider ~~reasonably expects~~discovers or confirms Student Data may have been disclosed in a data breach.

designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

(17)Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

(18)Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

(19)Protect the confidentiality of Student Data and Teacher Data at rest;

(20)Identify, report, and correct system flaws in a timely manner;

(21)Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22)Monitor system security alerts and advisories and take action in response; and

(23)Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB). For clarification, Provider's security program and documentation is based on ISO-27001/2, however, will be migrating to NIST 800/53 and CyberSecurity Framework. SOC-2 audits are based on this security program.

8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
   i. The estimated number of students and teachers affected by the breach, if any.

9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. ~~The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.~~.

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 ninety (90) days 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",** or, with reasonable notice to the Provider, other form of its choosing. 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".**

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."

12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an 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 LEA or its designee(s) 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 or its designee(s) 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 facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require ~~Contractor~~Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a