STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, NEW HAMPSHIRE, RHODE ISLAND, AND VERMONT

MA-ME-NH-RI-VT-DPA, Modified Version 1.0

PORTSMOUTH CHRISTIAN ACADEMY

and

QUALTRICS, LLC

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: Portsmouth Christian Academy, located at 20 Seaborne Drive, Dover, NH 03820 (the "**Local Education Agency**" or "**LEA**") and Qualtrics, LLC, located at 333 W. River Park Dr., Provo, UT 84604 (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, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three 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.

The designated representative for the Provider for this DPA is:

Name: Mark Creer Title: Deputy General Counsel

Address: 333 W. River Park Dr., Provo, UT 84604

Phone: 8013746682

Email: notice@qualtrics.com

The designated representative for the LEA for this DPA is:

Laurie Underwood, M.Ed, Director of Instructional Technology
Portsmouth Christian Academy
Email: lunderwood@pcaschool.org
20 Seaborne Drive, Dover, NH 03820
Phone: 603-742-3617 | ext. 141

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

PORTSMOUTH CHRISTIAN ACADEMY

By: Laurie Underwood
Laurie Underwood (Feb 2, 2024 08:36 EST)

Date: 2024-02-02

Printed Name: Laurie Underwood

Title/Position: Director of Technology

QUALTRICS, LLC

By:

Date: January 31, 2024

Printed Name: Mark Creer

Title/Position: Deputy General Counsel

STANDARD CLAUSES
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing 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"**. Notwithstanding anything contained herein to the contrary, LEA solely controls what Student Data is processed via the Cloud Service.

3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C".** Capitalized terms used herein but not otherwise defined in this DPA shall have the meanings ascribed to them in the Terms of Service. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. As between Provider and LEA, all Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall provide functionality for production systems that supports LEA's ability to correct, delete or anonymize Student Data from a Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, Provider will delete, anonymize, or correct any Student Data, or restrict its processing, in accordance with the LEA's instruction and Data Protection Law. 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 promptly notify LEA via e-mail and shall not respond to such request itself but instead askthe parent or individual to redirect its request to LEA.

3. **Intentionally Omitted**.

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 prohibited by applicable law or 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, regulations and legally binding rules pertaining to Student Data privacy and security, all as may be amended from time to time to the extent that Provider has not granted LEA the capability to comply with such law itself as set forth in this DPA and the Terms of Service or via the services or otherwise, and LEA shall comply with all applicable Data Protection Laws to the extent that it has the capability to comply with such laws as set forth in this DPA and the Terms of Service, or via the services or otherwise.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be processed only as necessary (a) to provide the Cloud Services to LEA or (b) as required to comply with applicable laws.

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(a) necessary to provide the Services, (b) directed or permitted by the LEA or this DPA, or (c) required by applicable law. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors or Provider's Affiliates, Provider agrees not transfer any 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 LEA who has provided prior written consent for such transfer. Prior to publishing any document that includes de-identified data 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**. During the Subscription Term, LEA can access its Student Data at any time. LEA may export, delete and retrieve its Student Data in a standard format. Export and retrieval may be subject to technical limitations, in which case Provider and LEA will find a reasonable method to allow LEA access to Student Data. Upon termination of the Service Agreement, Provider shall dispose of all applicable Student Data in accordance with its internal deletion policies (which shall not exceed a timeframe of six months). 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.

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; or (iv) as otherwise instructed by LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. On all applicable Order Forms, LEA may choose the United States as the data center region where its Student Data is permanently stored.

2.

Certifications and Audits.

2.1 Customer Audit. Customer or its independent third-party auditor reasonably acceptable to Qualtrics (which will not include any third-party auditors who are either a competitor of Qualtrics or not suitably qualified or independent) may audit Qualtrics' control environment and security practices relevant to Personal Data only if:

(a) Qualtrics has not provided sufficient evidence of its compliance with the Technical and Organizational Measures through providing either: (1) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (2) a valid SOC1-3 attestation report;

(b) a Personal Data Breach has occurred;

(c) an audit is formally requested by Customer's data protection authority; or

(d) Data Protection Law grants Customer a direct audit right, in which case Customer will only audit once in any 12-month period unless Data Protection Law requires more frequent audits.

2.2 Other Controller Audit. Any other Controller may assume Customer's rights under Section 6.1 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer. Customer will use all reasonable means to combine audits of all Controllers to avoid multiple audits unless the audit must be undertaken by the other Controller itself under Data Protection Law.

2.3 Scope of Audit. Customer will provide at least 60 days' advance notice of any audit unless Data Protection Law or a competent data protection authority requires shorter notice. The parties, acting reasonably and in good faith, will agree on the frequency and scope of any audits. Customer audits will be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer will provide the results of any audit to Qualtrics.

2.4 Cost of Audits. Customer will bear its costs of any audit and the cost of any third party unless such audit reveals a material breach by Qualtrics of this DPA, in which case Qualtrics shall bear the reasonable expenses of an audit. If an audit determines that Qualtrics has breached its obligations under the DPA, Qualtrics will promptly remedy the breach at its own cost.

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 state or Federal law relating to data security and directly applicable to the 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 to the DPA, contact information of an employee who LEA may contact 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) Intentionally Omitted.

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

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

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

ARTICLE VI: GENERAL OFFER OF TERMS

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

ARTICLE VII: MISCELLANEOUS

1. **Term**. The term of this DPA is as stated in the Order Form.
2. **Termination**. A party may terminate this DPA (along with the Service Agreement):
    a. upon 30 days' prior written notice of the other party's material breach of the Service Agreement or DPA unless the breach is cured during that 30-day period,
    b. as permitted under any other section in the Service Agreement (with termination effective 30 days after receipt of notice in each of these cases unless a different period is specified), or
    c. immediately if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors, or materially breaches Sections 11 or 12.6 of the Service Agreement.
3. **Refund and Payments**. For termination by LEA or an 8.1(c) of the Service Agreement termination by Provider, LEA will be entitled to:
    a. a pro-rata refund in the amount of the unused portion of prepaid fees for the terminated subscription calculated as of the effective date of termination, and
    b. a release from the obligation to pay fees due for periods after the effective date of termination.
4. **Effect of Expiration or Termination**. Upon the effective date of expiration or termination of the Service Agreement and DPA:
    a. LEA's right to use the Cloud Service and all Provider Confidential Information will end, and
    b. Confidential Information of the disclosing party will be retained, returned, or destroyed as required by the Service Agreement or applicable law.

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

6. **Priority of Agreements**. This DPA shall govern the treatment of Student Data. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between 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.

7. **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.

8. **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.

9. **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.

10. **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. Neither party will assign, delegate, or transfer the DPA and Service Agreement (or any of its rights or obligations) to any party without the prior written consent of the other party, except that either party may assign the Agreement to its Affiliates.

11. **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.

12. **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

Qualtrics XM

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

12

Category of Data	Elements	Check if Used by Your System
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	

Category of Data	Elements	Check if Used by Your System
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time.	

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

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

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

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

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

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

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

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

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

Student Data: Student Data includes any Personal Data processed by Provider provided by LEA or its users, students, or students' parents and its Subprocessors in connection with its provision of the Cloud Service, 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, except that which has been stripped of all direct and indirect identifiers (e.g., Analyses).

Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services. Student Data shall be processed as Personal Data in accordance with the Terms of Service, except to the extent there is a conflict with this DPA.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Terms of Service: Refers to the Terms of Service or General Terms and Conditions for Qualtrics Services found at https://www.qualtrics.com/terms-of-service/.

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

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. **Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and **Portsmouth Christian Academy** ("Originating LEA") which is dated 2024-02-02, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: notice@qualtrics.com.

Qualtrics, LLC

BY: _____ Date: January 31, 2024

Printed Name: Mark Creer Title/Position: Deputy General Counsel

2. **Subscribing LEA**

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

Subscribing LEA: (School District Name): _____

BY: _____ Date:_____

Printed Name: _____ Title/Position: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

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

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	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 processed by the Provider's Services may 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. LEA will not permit or request and Provider will not attempt to have any contact between students and Provider employees. If the Provider learns that a student of the LEA has contacted it relative to the Services, the Provider will refer the Student to the LEA (if the student has provided information to identify the LEA and if such notification is permitted by applicable law) and cease communication with the Student.
2. 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 processed by the Provider's Services may 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. Intentionally Omitted
2. LEA will not permit or request and Provider will not attempt to have any contact between students and Provider employees. If the Provider learns that a student of the LEA has contacted it relative to the Services, the Provider will refer the Student to the LEA (if the student has provided information to identify the LEA and if such notification is permitted by applicable law) and cease communication with the Student.
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 unless otherwise directed by the LEA. Publish means to disseminate to the public or to produce or release for distribution.
5. Intentionally Omitted
6. The parties agree if entered into or derived from its use of the Cloud Service by the LEA that the definition of Student Data in Exhibit "C" may include 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" may include information, to the extent entered into the Cloud Services by LEA or that LEA derives from its use of and stores in the Cloud Service, 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.

22

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and processed by the Provider's Services may 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. Intentionally Omitted
2. LEA will not permit or request and Provider will not attempt to have any contact between students and Provider employees. If the Provider learns that a student of the LEA has contacted it relative to the Services, the Provider will refer the Student to the LEA (if the student has provided information to identify the LEA and if such notification is permitted by applicable law) and cease communication with the Student.In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
3. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1 in Provider's role as a data processor.
4. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures, which program is outlined in Schedule 2 of Exhibit A to the Terms of Service. LEA has reviewed such measures and acknowledges that, as to the Cloud Service selected by LEA in the Services Agreement, the measures are appropriate taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing of Student Data.
5. 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 (to the extent known by the Provider and required by law, as it becomes available):
    - **i.** Information about what the Provider has done to protect individuals whose information has been breached
    - **ii.** Intentionally Omitted.
    - **iii.** Intentionally Omitted.

EXHIBIT "G"
Vermont

WHEREAS, the documents and data transferred from LEAs and processed by the Provider's Services may 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. Intentionally Omitted
2. 2. LEA will not permit or request and Provider will not attempt to have any contact between students and Provider employees. If the Provider learns that a student of the LEA has contacted it relative to the Services, the Provider will refer the Student to the LEA (if the student has provided information to identify the LEA and if such notification is permitted by applicable law) and cease communication with the Student.In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and processed by the Provider's Services may 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 Student Data processed 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." **If** entered into or derived from its use of the Cloud Service **by the LEA, "**Teacher Data" may include the following to the extent entered into the Cloud Services by LEA or that LEA derives from its use of and stores in the Cloud Service:

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. The LEA may provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I".**
3. Intentionally Omitted
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,…"
5. LEA will not permit or request and Provider will not attempt to have any contact between students and Provider employees. If the Provider learns that a student of the LEA has contacted it relative to the Services, the Provider will refer the Student to the LEA (if the student has provided information to identify the LEA and if such notification is permitted by applicable law) and cease communication with the Student.
6. Unless first anonymized, 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).

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, to the extent known by the Provider and as it becomes available:

    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. The Provider prohibits the LEA from providing the following: 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.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
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	

PCA_Qualtrics_VendorSigned

Final Audit Report 2024-02-02

Created:	2024-02-02
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAuv5KFt6HGxcrBF23ld3ZKzejcMdxKmk-

"PCA_Qualtrics_VendorSigned" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-02-02 - 12:05:26 PM GMT- IP address: 108.35.203.7

Document emailed to Laurie Underwood (lunderwood@pcaschool.org) for signature
2024-02-02 - 12:06:32 PM GMT

Email viewed by Laurie Underwood (lunderwood@pcaschool.org)
2024-02-02 - 1:35:14 PM GMT- IP address: 50.230.110.146

Document e-signed by Laurie Underwood (lunderwood@pcaschool.org)
Signature Date: 2024-02-02 - 1:36:16 PM GMT - Time Source: server- IP address: 50.230.110.146

Agreement completed.
2024-02-02 - 1:36:16 PM GMT