STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, NEW HAMPSHIRE AND RHODE ISLAND

MA-ME-NH-RI-NDPA, Standard Version 1.0

PORTSMOUTH SCHOOL DISTRICT

and

TEXTHELP, 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: Portsmouth School District, located at 29 Middle Rd., Portsmouth, RI 028 (the "**Local Education Agency**" or "**LEA**") and Texthelp, Inc., located at 500 Unicorn Park Dr, Woburn, MA 018C (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 a other regulated data exchanged between them as required by applicable laws and regulations, such as the Fan Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Priv: Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulatic and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respect 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 L 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 here incorporated by reference into this DPA in their entirety.

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

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will conti In the event there is conflict between the terms of the DPA and any other writing, including, but r limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this D shall control.

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

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

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be giv 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: __Karlene Feeney_____ Title: __Customer Success Manager__

Address: __500 Unicorn Park Drive Woburn, MA 01801_____

Phone: __888-248-0652_____

Email: __karlene@texthelp.com_____

The designated representative for the LEA for this DPA is:

Steven Costa, Director of Technology
Portsmouth School District
29 Middle Rd., Portsmouth, RI 02871
401-849-3700
costas@portsmouthschoolsri.org

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

PORTSMOUTH SCHOOL DISTRICT

By: _____

Date: ___7/19/2021_____

Printed Name: __Steven Costa_____

Title/Position: __Director of Technology_____

TEXTHELP, INC.

By: _____

Date: __July 16, 2021_____

Printed Name: __Jack Dolan_____

Title/Position: __President_____

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Stude Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulatio all as may be amended from time to time. In performing these services, the Provider shall be consider a School Official with a legitimate educational interest, and performing services otherwise provided the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use 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 confli definitions used in this DPA shall prevail over terms used in any other writing, including, but not limit to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

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

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by whicl parent, legal guardian, or eligible student may review Education Records and/or Student Data corr erroneous information, and procedures for the transfer of student-generated content to a persor account, consistent with the functionality of services. Provider shall respond in a reasonably tim manner (and no later than forty five (45) days from the date of the request or pursuant to the time frar required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LE, request for Student Data in a student's records held by the Provider to view or correct as necessary. the event that a parent of a student or other individual contacts the Provider to review any of the Stude Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, w 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 sh at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Stude Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesti Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Servic the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unle 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 functic for the Provider in order for the Provider to provide the Services pursuant to the Service Agreeme whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the teri 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 w 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 acce LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized acce:

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, a 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 uniq identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in t 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 ha access to Student Data to comply with all applicable provisions of this DPA with respect to the Stude Data shared under the Service Agreement. Provider agrees to require and maintain an appropri; confidentiality agreement from each employee or agent with access to Student Data pursuant to t Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Stude Data or any portion thereof, including without limitation, user content or other non-public informati

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggrega summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoe or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to t 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-Identif Data may be used by the Provider for those purposes allowed under FERPA and the following purpos (1) assisting the LEA or other governmental agencies in conducting research and other studies; and research and development of the Provider's educational sites, services, or applications, and demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customi student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any requ by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identificatii and (b) prior written notice has been given to the LEA who has provided prior written consent for su transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider sh 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 mechani for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of t date of said request and according to a schedule and procedure as the Parties may reasonably agr Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student D shall not extend to Student Data that had been De-Identified or placed in a separate student accou pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of wh is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written requ or notice is required on the part of either party prior to the disposition of Student Data described in Exhi "D.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) infor influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guard or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provi from using Student Data (i) for adaptive learning or customized student learning (including generat personalized learning recommendations); or (ii) to make product recommendations to teachers or L employees; or (iii) to notify account holders about new education product updates, features, or servi 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 Stat Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written requ from the LEA with at least ten (10) business days' notice and upon the execution of an appropri confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures tl are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provic and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provide facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delive 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 design to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, modification. The Provider shall adhere to any applicable law relating to data security. The provider sh implement an adequate Cybersecurity Framework based on one of the nationally recognized standar set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framewc must be detailed in an attachment. Additionally, Provider may choose to further detail its secur programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "** Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who L 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 tl compromises the security, confidentiality or integrity of the Student Data maintained by the Provider t Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incide unless notification within this time limit would disrupt investigation of the incident by law enforceme In such an event, notification shall be made within a reasonable time after the incident. Provider sh follow the following process:

    (1) The security breach notification described above shall include, at a minimum, the followi 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 he been the subject of a breach.
        iii. If the information is possible to determine at the time the notice is provided, then eith (1) the date of the breach, (2) the estimated date of the breach, or (3) the date rar within which the breach occurred. The notification shall also include the date of t notice.
        iv. Whether the notification was delayed as a result of a law enforcement investigation 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 determi at the time the notice is provided.

    (2) Provider agrees to adhere to all federal and state requirements with respect to a data brez related to the Student Data, including, when appropriate or required, the required responsibilit 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 refle best practices and is consistent with industry standards and federal and state law for respond to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Stud< Data or any portion thereof, including personally identifiable information and agrees to prov 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 guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate wi 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 here as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhib 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 writt consent so long as the Service Agreement has lapsed or has been terminated. Either party may termina this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all 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 t privacy protections, including those found in FERPA and all applicable privacy statutes identified in tl DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DI shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and t Supplemental State Terms, the Supplemental State Terms will control. Except as described in tl 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 Parti relating to the subject matter hereof and supersedes all prior communications, representations, agreements, oral or written, by the Parties relating thereto. This DPA may be amended and t observance of any provision of this DPA may be waived (either generally or in any particular instance a either retroactively or prospectively) only with the signed written consent of both Parties. Neither failu nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate a: waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclu 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 such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidati the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction sh not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding t foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to su jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecti 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 ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LA PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO T STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF (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 Provic in the event of a merger, acquisition, consolidation or other business reorganization or sale of all substantially all of the assets of such business In the event that the Provider sells, merges, or otherw disposes of its business to a successor during the term of this DPA, the Provider shall provide writt notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Su notice shall include a written, signed assurance that the successor will assume the obligations of the D and any obligations with respect to Student Data within the Service Agreement. The LEA has the author to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, otherwise disposing of its business.

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

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed a; waiver of any such right and both parties reserve the right to exercise any such right from time to tin as often as may be deemed expedient.

Read&Write's family of literacy software makes the web, documents and files more accessible - any time, any place, and on any platform. It's great for people with dyslexia and other learning difficulties or anyone whose first language isn't English. From reading on-screen text aloud to researching and checking written work, Read&Write makes lots of everyday tasks easier. It's a big confidence booster for anyone who needs a little extra help with their reading and writing, at school or in the workplace.

Snapverter is an easy to use add-on for Read&Write for Google Chrome™ that transforms classroom papers and files into readable PDF documents for easy sharing and reading aloud via Google Drive. Pi any inaccessible file to convert - or just grab your smartphone and snap a photo of paper documents. Then share converted files with students and other teachers on any device - PCs, Macs, Chromebook or tablets. **PDF Reader,** when paired with Snapverter, teachers and students can easily identify and OCR inaccessible PDFs. Ensuring that students have access to tools such as text to speech.

EquatIO® lets everyone create mathematical equations, formulas and more on their computer or Chromebook. Input's easy. Type, handwrite, or dictate any expression, with no tricky coding or maths languages to master. There's a huge library of ready-made expressions to save you time, from simple formulas to complex functions. And when you're done, just add the math to your document with a click.

Fluency Tutor for Google makes reading aloud more fun and satisfying for students who need some extra support. Easy to use with a sleek new look, our software allows students to record themselves reading and then share that content with their teacher - away from the pressures of reading aloud in the classroom environment. It's ideal for schools using G Suite for Education as our Chrome app integrates seamlessly with Google Classroom and Google Drive. And since it works with any online content, it's the perfect complement to other existing teacher approaches.

WriQ is an extension for Google Docs that grades papers digitally - saving more time for other precio classroom activities. It's faster, more accurate and consistent than subjective, pen and paper manual assessment - giving clear visibility of progress over time against peers and standardized norms. WriQ provides much needed comparable insights on writing levels within a school, district or at a state/national level. Making it easier to allocate invaluable district resources, progress student literac and improve writing performance.

SpeechStream is a cloud-based literacy and language support. It helps publishers of online learning a assessments to make content more accessible. And it supports online learners to learn and achieve independently.

Texthelp Study Skills: Texthelp Highlighting Tools: Select, Highlight, and Group Content Together for Review and Learning.

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:	
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	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	

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	X
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	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)	
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.	X
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	

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. Provider will immediately notify LEA if this designation is no longer	

EXHIBIT "C"
DEFINITIONS

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

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

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

Operator: means the operator of an internet website, online service, online application, or mobile application w actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operat an internet website, online service, online application, or mobile application that has entered into a signed, writt agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of tl 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 servic including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the D the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statut

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

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

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its use students, or students' parents/guardians, that is descriptive of the student including, but not limited 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, discipli records, videos, test results, special education data, juvenile dependency records, grades, evaluations, crimir records, medical records, health records, social security numbers, biometric information, disabiliti socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliation religious information, text messages, documents, student identifiers, search activity, photos, voice recordin; geolocation information, parents' names, or any other information or identification number that would provi information about a specific student. Student Data includes Meta Data. Student Data further includes "persona identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Stude Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, a local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed the Provider pursuant to the Services. Student Data shall not constitute that information that has be anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as t "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analyti 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 Provide General Offer of Privacy Terms.

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

Third Party: The term "Third Party" means a provider of digital educational software or services, including clou based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when us 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 i 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 "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Portsmouth School Distr** ("Originating LEA") which is dated <u>07/14/2021</u>, to any other LEA ("Subscribing LEA") who accepts tl General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend oi to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as pri term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribi LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in t applicable privacy statutes; (2) a material change in the services and products listed in the originating Servi 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: Karlene@te

_____.

TEXTHELP, INC.
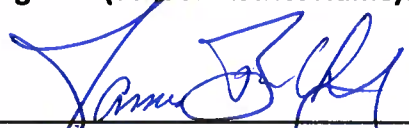
BY: _____ Date: July 16, 2021 _____

Printed Name: Jack Dolan _____ Title/Position: President _____

2. Subscribing LEA

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

Subscribing LEA: (School District Name): Regional School Unit 25 _____

BY: _____ Date: 3/18/2022 _____

Printed Name: James Boothby _____ Title/Position: Superintendent

DESIGNATED REPRESENTATIVE OF LEA:

Name: James Boothby _____

Title: Superintendent _____

Address: 62 Mechanic St. Bucksport ME 04416

Telephone Number: (207) 469-7311 _____

Email: jim.boothby@rsu25.org _____

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 Priva
Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which c
protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecur
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
X	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 subje
to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General La
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 Servic
provided conform to the requirements of the privacy laws referred to above and to establish implementi
procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety f
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 ir
   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 sever 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 Specia 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 c 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 ir 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"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subje 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, a 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 Servic provided conform to the requirements of the privacy laws referred to above and to establish implementi procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety 1 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 state in the Service Agreement."

2. All employees of the Provider who will have direct contact with students shall pass criminal backgroun 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 contai 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 informatic 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, o 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 fe may be required to be paid to the consumer reporting agencies.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subje
to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; I
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 Servic
provided conform to the requirements of the privacy laws referred to above and to establish implementi
procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety 1
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 Dat
    described in the Schedule of Data, attached hereto as **Exhibit "I"**.
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) u

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 b' organizational systems) at the external boundaries and key internal boundaries of organizational systems;

(18)Deny network communications traffic by default and allow network communications traffi 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) FedRAN (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Securit (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 th 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 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:

    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, a 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 Unitec States.

Category of Data	Elements	Check if by yo syste
EXHIBIT "I" – TEACHER DATA		
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	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	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	

TextHelp_PortsmouthRI_VendorSigned

Final Audit Report   2021-07-19

Created:	2021-07-16
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA6nxwBxZTRsrGKc_0-XhVuXVB6CgKZiGp

"TextHelp_PortsmouthRI_VendorSigned" History

📄 Document created by Ramah Hawley (rhawley@tec-coop.org)
2021-07-16 - 9:26:55 PM GMT- IP address: 100.1.115.187

📩 Document emailed to Steven Costa (costas@portsmouthschoolsri.org) for signature
2021-07-16 - 9:27:39 PM GMT

📄 Email viewed by Steven Costa (costas@portsmouthschoolsri.org)
2021-07-17 - 12:00:59 PM GMT- IP address: 66.102.8.5

✍ Document e-signed by Steven Costa (costas@portsmouthschoolsri.org)
Signature Date: 2021-07-19 - 12:32:37 PM GMT - Time Source: server- IP address: 131.109.73.242

✅ Agreement completed.
2021-07-19 - 12:32:37 PM GMT