DISCLAIMER for MOREnet's Missouri NDPA

The Student Data Privacy Consortium ("SDPC") has developed the "National Data Privacy Agreement" ("NDPA"). The SDPC formed a DPA Project Team consisting of individuals from schools, state organizations, marketplace providers, and legal organizations to develop this standard template that addresses the common student data privacy issues that need to be addressed in contracts with vendors that handle student data (see https://privacy.a4l.org/national-dpa) .

The Missouri Research and Education Network (MOREnet), a department of the University of Missouri System, has joined the SDPC and has established the Missouri Student Privacy Alliance, which all MOREnet Member schools are eligible to join. As such, MOREnet is making the NDPA available to its members as a resource for informational purposes only; it should not be relied on as legal advice. While MOREnet believes this is a well-developed tool, MOREnet makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in the NDPA. ***Should you elect to use the NDPA as a resource, we strongly encourage you to obtain your own legal counsel in drafting and/or entering into vendor agreements that pertain to student data.*** There may be unique needs of your school or systems that need to be addressed or other provisions that you believe are critical, which can be set forth in Exhibit H.

Exhibit G is intended to include any specific Missouri laws that apply to student data, which may be applicable to your school. However, laws are constantly subject to change and new ones can be enacted. Additionally, there may be other laws or National or Missouri guidelines or standards that are applicable to your school with which you must comply. ***MOREnet is not representing that the laws set forth in Exhibit G are the only laws, guidelines, and/or standards which should be included, as applicable to you and/or to a specific vendor agreement***. Your own legal counsel should be consulted and any additional terms you may require should be added to Exhibit H.

STANDARD STUDENT DATA PRIVACY AGREEMENT

MO-NDPA Standard Version 1.5

Rockwood R-VI School District

and

[NAME OF PROVIDER]

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:

Rockwood R-VI School District, located at 111 E. North St., Eureka, MO 63025 (the "**Local Education Agency**" or "**LEA**") and

Helper Helper located at [Street, City, State] (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, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**
   - ☐ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

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

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

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

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

The designated representative for the LEA for this DPA is:

Name: Deborah Ketring Title: Chief Information Officer

Address: 111 E. North St., Eureka MO 63025

Phone: (636)733-1103 Email: ketringdeborah@rsdmo.org

The designated representative for the Provider for this DPA is:

Name: Title:

Address:

Phone: Email:

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

LEA [School District Name]

By: Date:

Printed Name: Deborah Ketring Title/Position: Chief Information Officer

[Insert Name of Provider]

By: Date:

Printed Name: Title/Position:

STANDARD CLAUSES
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

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

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of allStudent Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **"Directive for Disposition of Data"** form, a copy of whichis attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit"D"**.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

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

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

i. The name and contact information of the reporting LEA subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

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

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

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

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

ARTICLE VI: GENERAL OFFER OF TERMS

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

ARTICLE VII: MISCELLANEOUS

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

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

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between **Exhibit "H"**, the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

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

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

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

EXHIBIT "A"
DESCRIPTION OF SERVICES

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	

Category of Data	Elements	Check if Used by Your System
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	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	

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

EXHIBIT "C"
DEFINITIONS

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

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

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

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

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

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

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

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

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to,

information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

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

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

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

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

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

Rockwood Provider to dispose of data obtained by Provider pursuant to the terms of theService Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[**Insert categories of data here**]

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

2. Nature of Disposition

_X_____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:

_X_____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 [**Insert Name of Originating LEA**] ("Originating LEA") which is dated [**Insert Date**], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:_____.

[NAME OF PROVIDER]

BY:_____ Date: _____

Printed Name:_____ Title/Position: _____

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 [**Insert Name of Originating LEA**] and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

[**Insert Name of Subscribing LEA**]

BY:

_____ Date:_____

Printed Name:_____ Title/Position:_____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

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

Cybersecurity Frameworks

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

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

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

EXHIBIT "G"

EXHIBIT "G" – Supplemental NDPA State Terms for Missouri

Version: October 2020

A. DATA BREACH

In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student's family member, Provider shall notify LEA within five (5) business days. The notice shall include:

1. Details of the incident, including when it occurred and when it was discovered;
2. The type of personal information that was obtained as a result of the breach; and
3. The contact person for Provider who has more information about the incident.

"*Breach*" shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

"*Personal information*" is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:

1. Social Security Number;
2. Driver's license number or other unique identification number created or collected by a government body;
3. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
4. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account;
5. Medical information; or
6. Health insurance information.

EXHIBIT "H"

Additional Terms or Modifications

As used in this Exhibit H, the term "Agreement" shall refer to the DPA and the Service Agreement collectively. LEA and Provider agree to the following additional terms and modifications to the DPA:

1. Article IV, Section 3 of the DPA, Provider Employee Obligation, is hereby supplemented by adding three new sentences to the end of the Section to read as follows:
   Provider shall require that its employees, contractors, and agents who have access to Student Data pursuant to the DPA complete periodic security training. Provider shall keep true and complete records of any and all Student Data received, exchanged and shared between and amongst its employees, agents, and contractors and permit LEA to access such records upon request. Provider shall also outline for LEA the steps and processes that Provider will take to prevent post-employment data breaches by Provider employees after their employment with Provider has been terminated.
2. Article IV, Section 4 of the DPA, No Disclosure, is hereby supplemented by adding one new sentence to the beginning of the Section to read as follows:
   Provider shall exclusively limit its employees, contractors, and agents' access to and use of Student Data to those individuals who have a legitimate need to access Student Data in order to provide services to the LEA.
3. The second sentence of Article IV, Section 7 of the DPA, Advertising Limitations, is hereby deleted in its entirety and one new sentence is inserted to read as follows:
   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) from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.
4. The first sentence of Article V, Section 1 of the DPA, Data Storage, is hereby deleted in its entirety and replaced with one new sentence to read as follows:
   Student Data shall be stored within the United States.
5. Article V, Section 3 of the DPA, Data Security, shall be supplemented by adding three new sentences to the end of the Section to read as follows:
   In conducting data transactions and transfers with the LEA, Provider shall ensure that all such transactions and transfers are encrypted. Provider represents and warrants that all of its data portals are secured through the use of verified digital certificates. Provider shall provide LEA with a data inventory that inventories all data fields and delineates which fields are encrypted within Provider's platform maintaining collected Student Data.
6. Article V, Section 4 of the DPA, Data Breach, is hereby modified as follows:
   a. The first sentence of Section 4 shall be deleted in its entirety and one new sentence is inserted to read as follows:
      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 thirty-six (36) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement.

b. One new subsection (6) shall be added to this Section 4 to read as follows:

Notwithstanding the foregoing, if a data breach is caused by the acts or omissions of Provider or its agents, employees, or contractors, Provider shall be responsible for the timing, content, and costs of any legally-required notifications. Furthermore, Provider is also responsible for the costs of investigating a breach, as well as the payment of actual, documented costs including reasonable attorneys' fees, audit costs, fines, and other fees imposed against LEA as a result of any data breach caused by the acts or omissions of Provider or is agents, employees, or contractors. With respect to any data breach which is not due to the acts or omissions of Provider or its agents, employees, or contractors, Provider shall nevertheless reasonably cooperate in the LEA's investigation and third-party notifications, if any, at the LEA's direction and expense.

7. Article VII, Section 1 of the DPA, Termination, is hereby deleted in its entirety and one new Section is inserted to read as follows:

Termination. LEA may terminate this DPA at any time, for any reason, by giving at least ten (10) days' notice in writing to Provider. This DPA shall automatically terminate upon the latter of (i) termination or expiration of the Service Agreement between LEA and Provider; or (ii) LEA's receipt of written confirmation from Provider that all of the Student Data provided by LEA to Provider, or created or received by Provider, in performance of the Service Agreement has been destroyed by Provider or returned to LEA. Either Party may terminate this DPA and any Service Agreement if the other Party breaches any terms of this DPA upon written notice to the non-breaching Party.

8. The second sentence of Article VII, Section 3 of the DPA, Priority of Agreements, is hereby deleted in its entirety and one new sentence is inserted to read as follows:

In the event there is conflict with respect to the treatment of Student Data 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.

9. The last sentence of Article VII, Section 7 of the DPA, Successors Bound, is hereby deleted in its entirety and one new sentence is inserted to read as follows:

The LEA has the authority to terminate the DPA and the Service Agreement in its sole discretion if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

10. Exhibit C of the DPA, Definitions, is hereby amended as follows:

a. One new defined term and definition shall be added to read as follows:

Data Breach: For purposes of this DPA, the term "data breach" means actual evidence of a confirmed unauthorized acquisition of, access to, or unauthorized use of any Student Data and/or Educational Records.

b. The definition of the term Service Agreement shall be amended to read as follows:

Service Agreement: Refers to the Contract, Purchase Order, Terms of Service, or Terms of Use between Provider and LEA.

11. The first sentence of Exhibit G, Section A of the DPA, Data Breach, is hereby deleted in its entirety and one new sentence is inserted to read as follows:

In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student's family member, Provider shall notify LEA in writing within three (3) business days.

12. **Indemnity.** Provider agrees to indemnify, defend, and hold harmless the LEA, its Board of Education, officers, directors, employees, representatives, agents,

successors, and assigns from, against, and in respect to any and all claims, losses, damages, suits, or liabilities, including costs and attorneys' fees, for damages incurred or suffered, directly or indirectly, arising from or relating to the acts and/or omissions of Provider and/or its employees, contractors, or agents, in connection with providing the services, as is contemplated under this Agreement.

13. **Insurance**. At all times during the term of the Agreement, Provider shall maintain, at its sole cost and expense, insurance coverage as follows: (i) Commercial General Liability insurance in an amount not less than $1,000,000 per occurrence and $2,000,000 in aggregate; and (ii) Cyber Security insurance in an amount not less than $1,000,000 per occurrence and $2,000,000 in aggregate. LEA shall be named as an additional insured on the commercial general liability policy and all such insurance coverage shall be primary and non-contributory with respect to any insurance maintained by LEA. Copies of Provider's certificates of insurance showing the required coverage shall be provided to LEA upon execution.
14. **Force Majeure.** If either party is prevented from performing any of its obligations due to any cause which is beyond the non-performing party's reasonable control, including fire, explosion, flood, epidemic/pandemic or other acts of God; acts, regulations, or laws of any government; strike, lock-out or labor disturbances; or failure of public utilities or common carriers (a "Force Majeure Event"), such non-performing party shall not be liable for breach of this Agreement with respect to such non-performance to the extent any such non-performance is due to a Force Majeure Event. Such non-performance will be excused for three months or as long as such event shall be continuing (whichever occurs sooner), provided that the non-performing party gives immediate written notice to the other party of the Force Majeure Event.
15. **Disputes.** To the extent allowed by applicable law, any controversy or claim arising out of or relating to this Agreement or any breach thereof, may be settled by informal mediation with the parties subject to this Agreement.
16. **Compliance with Laws and LEA Board Policy.** Provider, at Provider's sole cost, shall comply with applicable LEA Board Policy as well as all present and future laws, ordinances, rules, regulations, including but not limited to: the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99); Protection of Pupil Rights Amendment ("PPRA") (20 U.S.C. § 1232h; 34 CFR Part 98), all of them which may be in effect or amended from time to time, including any successor statute and its implementing regulations and rules. In the event of a conflict between this Agreement and federal and state confidentiality and privacy laws ("Confidentiality Laws"), the Confidentiality Laws shall control. In the event of a conflict between FERPA and any other Confidentiality Laws, FERPA will control absent clear statutory authority on controlling law.
17. **Children's Online Privacy Protection Act.** The parties recognize and agree that with respect to the Children's Online Privacy Protection Act ("COPPA"), the LEA gives its consent to Provider on behalf of parents of children from whom any personal information shall be gathered, as contemplated under the Agreement. As the agreement only contemplates the potential collection of personal information from children under the age of thirteen (13) for educational purposes, for the use and benefit of the school, and for no other commercial purpose, the parties recognize that COPPA does not require that the Provider obtain consent from parents directly. As such, notwithstanding any other provision in the Agreement to the contrary, the LEA shall not be responsible under the terms of this Agreement to collect consent from individual parents.

18. **Federal Work Authorization Program.** (APPLICABLE IF THE CONTRACT IS FOR AN AMOUNT GREATER THAN $5,000) Prior to commencement of any work contemplated under this Agreement, Provider shall provide to the LEA a sworn affidavit and other sufficient documentation to affirm its enrollment and participation in the Federal Work Authorization Program. Federal Work Authorization Program means the eVerify program maintained and operated by the United States Department of Homeland Security and the Social Security Administration, or any successor program. Provider shall also provide the LEA a sworn affidavit affirming that it does not knowingly employ any person who is an unauthorized alien in connection with the contracted services.

19. **Background Checks.** (APPLICABLE IF ANY PROVIDER EMPLOYEE WILL EVER HAVE ACCESS TO STUDENT DATA) Before employment of any employee, contractor, subcontractor, consultant or subconsultant who is an individual for work on the services set forth in this Agreement, the Provider shall conduct background checks through all appropriate state agencies and any other background checks as may be standard for entities providing services to public schools, including without limitation, a thorough review of the list of registered sex offenders as provided by the County Sheriff's Department, the Federal Bureau of Investigation's criminal history files, the Missouri Highway Patrol's criminal history database and sexual offender registry, the Family Care Safety Registry, or the central registry of child abuse and neglect of the Missouri Children's Division; and any such individual who does not pass such background check as determined by the LEA in its sole discretion shall not be permitted to enter the premises where the services are being performed or any other school LEA property or to work on the services under this Agreement. The Provider shall include all of these requirements in its contracts with their subcontractors and suppliers.

20. **Drugs and Alcohol.** (APPLICIABLE IF ANY PROVIDER EMPLOYEE WILL EVER BE ON SCHOOL PROPERTY) The Provider shall be responsible to the LEA for acts and omissions of the Provider's employees, subcontractors and their agents and employees, and other persons or entities performing portions any work contemplated under this Agreement for, or on behalf of, the Provider or any of its subcontractors. As part of that responsibility, Provider shall enforce the LEA's alcohol-free, drug-free, tobacco-free, harassment-free and weapon-free policies and zones, which will require compliance with those policies and zones by Provider's employees, subcontractors, and all other persons carrying out the Agreement.

21. **No Boycott of Israel**. (APPLICABLE IF THE CONTRACT IS FOR AN AMOUNT GREATER THAN $100,000) All parties to this Agreement certify that they are not currently engaged in and shall not, for the duration of the contract, engage in a boycott of goods or services from the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel.

22. **Immunity Retention**. LEA does not intend to, nor shall any provision of this Agreement be construed in such a way as to, waive or terminate the statutory or common law immunities enjoyed by LEA, or its Board of Education, officers, directors, employees, representatives, agents, successors, or assigns. LEA shall retain all immunities, including those immunities contained within Missouri Revised Statute § 537.600 et.seq.