STANDARD STUDENT DATA PRIVACY AGREEMENT

UT-NDPA-Vendor-Specific

AGREEMENT TYPE

Provo City School District

LEA

and

Slate Solutions, Inc DBA "Transeo"

Provider

03/29/2022

Date

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:
[Provo City School District], located at [280 W 940 N, PROVO, UT, 84604] (the "**Local Education Agency**" or "**LEA**") and [Slate Solutions, Inc DBA "Transeo"], located at [954 S Madison St., Hinsdale, IL 60521] (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 years. Exhibit E will expire 3 years from the date the original DPA was signed.

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

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

The designated representative for the LEA for this DPA is:

Name: Clint Smith Title: Data Privacy Coordinator

Address: 280 W 940 N, PROVO, UT, 84604

Phone: 801-374-4859 Email: clints@provo.edu

The designated representative for the Provider for this DPA is:

Name: Patrick Woodring Title: VP, Finance & Business Operations

Address: 954 S Madison St., Hinsdale, IL 60521

Phone: 877-300-3793 Email: patrick@gotranseo.com

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

LEA [Provo City School District**]**

By: Clint Smith Digitally signed by Clint Smith Date: 2022.03.30 11:09:20 -06'00' Date: 03/29/2022

Printed Name: Clint Smith Title/Position: Data Privacy Coordinator

Provider [Slate Solutions, Inc DBA "Transeo"**]**

By: Rippling Identity (Patrick's MacBook Air) Digitally signed by Rippling Identity (Patrick's MacBook Air) Date: 2022.03.29 16:41:44 -04'00' Date: 03/29/2022

Printed Name: Patrick H Woodring Title/Position: VP, Finance & Business Ops

STANDARD CLAUSES
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

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

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

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 all Student 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 which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D.

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

ARTICLE V: DATA PROVISIONS

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

2. **Audits.** No more than once a year, or following unauthorized access, 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

Transeo is a multifaceted educational technology platform that augments the student and administrative experience in order to create a comprehensive tool that allows schools to support every individual student through community engagement tracking, workplace learning, and post graduation pathway planning.

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: Each district can decide additional data points	✔
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: Each district is able to send any data points they'd like and Transeo will store it and allow them to report on it. By default, the only required student information that each district must provide is the student's first and last name and the student's email address. Many districts opt to send no more data than that, but some choose to send data pieces described by the checked boxes above.	✔
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

[**Insert LEA Name**] _____Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[**Insert categories of data here**]_____

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

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[**Insert or attach special instructions**]_____

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [**Insert Date**]_____

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and [Provo City School District] ("Originating LEA") which is dated [03/29/2022], 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: patrick@gotranseo.com.

[Slate Solutions, Inc DBA "Transeo"]

BY: Rippling Identity (Patrick's MacBook Air) Digitally signed by Rippling Identity (Patrick's MacBook Air) Date: 2022.03.29 16:42:28 -04'00' Date: 03/29/2022

Printed Name: Patrick H Woodring Title/Position: VP, Finance & Business Operations

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 [Provo City School District] and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

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

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

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

EXHIBIT "G"

Supplemental SDPC State Terms for [State]

Version _____

[The State Supplement is an ***optional*** set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit "H"** in this proposed structure).]

[THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK]

EXHIBIT "H"

Additional Terms or Modifications

Version 1

LEA and Provider agree to the following additional terms and modifications:

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

No modification of terms. Attached below is Transeo's full security policy. Transeo treats cybersecurity with the utmost priority and we will review the security frameworks outlined in Exhibit "D" to ensure compliance with those that are most applicable to our services.

Organizational Security Policy

The Transeo Organizational Security Policy (referred to as “policy”) is a set of guidelines for all Transeo employees, contractors, and partners (collectively, “individuals”) regarding usage of technology vendors and platforms. It is a company-wide expectation that all members follow this guide and adhere to the policies within. This document also includes an acceptable use policy for Transeo technology usage.

External Vendors

Beginning May 1st, 2020, all external vendors must be vetted and approved by the Transeo technology department. This process is not meant to be a roadblock to new services being implemented, but is instead meant to encourage detailed research before purchasing decisions. Additionally, implementing the following controls allows Transeo to maintain its data security integrity as we grow. **No Transeo employee or team is permitted to contract or sign up with new external vendors without the approval of the Transeo technology team.**

When evaluating a new external vendor, ask (and report) the following questions:

1. What type of company data is required to use this vendor?
2. Do they offer single sign on as an authentication method?
3. How is payment information entered and stored? Do they use a vendor like Stripe to handle this information?
4. Have you contacted Jimmy about a Rippling integration?

Single sign on is a critical feature of new external vendors approved for Transeo use. If this feature is not offered, please have a discussion internally with the Transeo technology team about other options, as we might be able to set up a secure VPN or Cloudflare Access portal.

Any service that requires your email address or any other company information to sign up is classified as an external vendor. See below for a non-exhaustive list of existing relationships with external vendors:

1. Salesforce
2. Slack
3. CHAOSSEARCH
4. Zoom

Internal Applications

Internal applications consist of services that have been built by the Transeo engineering department for use by Transeo employees. These internal applications are protected by

Cloudflare Access. You can view a list of available Transeo internal applications by visiting https://gotranseo.cloudflareaccess.com. Examples of internal applications include:

1. Trns.io link shortener
2. Metabase
3. Transeo account impersonation
4. Homeroom
5. Kubernetes dashboard

All of these services require that you authenticate with your Transeo email account before proceeding.

VPN

Members of the engineering department who need access to any of the following services must use a Transeo-supplied VPN:

1. Kubernetes Dashboard
2. Grafana Dashboard
3. Kubectl command line tools
4. Read-only database access
5. Read/write database access
6. Redis instances
7. EC2 instances

Additionally, engineers accessing legacy Serve accounts via the Homeroom interface must use their dedicated IP address. This policy does not apply to Transeo 2.0 admin impersonations. Please see “Internal Applications” for more information.

Transeo has a corporate account with NordVPN and will assign you a dedicated IP address for your use. After this IP has been assigned please contact Jimmy to add the IP to the whitelist for the appropriate services. Transeo reserves the right to collect, observe, and retain all traffic routed through a Transeo-supplied VPN.

Company Devices

Company devices provided for work usage as expected to comply with the acceptable use policy. Please see the policy for more details.

Traveling Internationally

When traveling internationally, either for Transeo-related business or for personal reasons, please be aware that you may be required to unlock your phone or other computing device at

customs, possibly exposing sensitive company data. It is of the utmost importance that you do your best to minimize this possibility.

What's a work device? Anything you have company data on: your laptop where you work with Transeo source code or data; your tablet where you read Transeo email; your phone where you view Transeo data; etc.

The quick summary of our policies regarding international travel is don't travel with work data. If you don't need a work device for your travel purposes, don't bring it. Wipe Transeo data from your device before traveling and restore it after.

Before you travel, complete the following items:

1. Let Jimmy and Don know that you are traveling internationally.
2. Put Jimmy and Don on speed dial so that you can access one or both of us in the event that Customs and Border Protection requires access to your work device.
3. If you use an email app rather than Gmail in your browser, remove your @gotranseo.com email address from it.
4. Clear browser cookies, logging you out of all work sites.
    - Laptops: Clear cookies in Chrome, Safari, etc.
    - iOS: Settings > Safari > Clear History and Website Data
    - Android: Chrome > Settings > Privacy > Clear browsing data. Check Cookies and site data; uncheck all the other items. > Clear data.
5. Transeo source code
    - Make an encrypted archive of your Transeo git repos so you can download and restore it after you're through customs.
    - Delete all Transeo source code from your laptop.
6. Other sensitive documents
    - Same deal as source code. Make an encrypted backup and remove from your laptop.
7. Touch ID (optional)
    - Unlocking your device can be compelled at US border crossings, but other countries may be less intrusive, so it may make sense to make your device a little harder to unlock. Disable Touch ID on your phone, tablet, and laptop. Require a passcode/password to unlock.

Finally, please use common sense when traveling with work devices. Do not access or update financial information on public wifi networks; don't allow your plane neighbor to view Transeo source code because they're interested; don't enter a password in a public setting. If any travel policies don't make sense, contact Jimmy for more information.

Single Sign On

Use single sign on (SSO) through your Transeo G Suite account to access vendors and services. This ensures that all accounts are provisioned correctly. If the service provider you want to use does not offer SSO, please contact the Transeo technology department to set up a secure VPN or Cloudflare Access portal.

Additionally, all external vendors must be provisioned using Rippling. If an external vendor was created without Rippling please contact the Transeo technology department to have the service added.

Two Factor Authentication

All individuals are required to use two factor authentication on their Transeo G Suite accounts. Two factor authentication is not enforced on any other services, but is **highly recommended.** If your Transeo account for an external vendor is hacked or compromised, two factor authentication was available, and you did not set it up as recommended in these policies you may be held personally responsible for data or information loss.

Passwords

Passwords used for external providers should comply with the following guidelines:

1. Does not include any of the following words: Transeo, Jobs, Journey, Serve, 2020, Slate Solutions.
2. Is not used for multiple services
3. Includes a number, a letter, a special character, and is at least 8 characters in length

Transeo recommends the usage of a password management system like Rippling RPass for secure storage of credentials.

Most importantly, all individuals are prohibited from storing passwords in plaintext for convenience. This includes but is not limited to:

1. Physical notes (Post-Its, notepads, etc)
2. Google documents
3. Google spreadsheets
4. Slack messages

To share a password with a team member securely, please ping it to them in Slack, or ideally add them as a member inside of the software so that they can create their own set of credentials.

Technology Acceptable Usage Policy

This Acceptable Usage Policy covers the security and use of all Transeo information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Transeo employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Transeo's business activities worldwide, and to all information handled by Transeo relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated by Transeo or on its behalf.

Computer Access Control – Individual's Responsibility

Access to the Transeo IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Transeo IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any Transeo IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Transeo's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorized changes to Transeo's IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non-Transeo authorized device to the Transeo network or IT systems.
- Store Transeo data on any non-authorized Transeo equipment.
- Give or transfer Transeo data or software to any person or organization outside Transeo without the authority of Transeo.

Managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Use of Transeo internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Transeo in any way, not in breach of any term and condition of employment, and does not place the individual or Transeo in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Transeo considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Transeo, alter any information about it, or express any opinion about Transeo, unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Make official comments through the internet or email on behalf of Transeo unless authorized to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect Transeo devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of information, Transeo enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided (for example, secure print on printers).
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Transeo remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption is required via the Rippling MDM.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices
Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Transeo authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software
Employees must use only software that is authorized by Transeo on Transeo's computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on Transeo computers must be approved by the Transeo IT department.

Individuals must not:

- Store personal files such as music, video, photographs or games on Transeo IT equipment.

Telephony (Voice) Equipment Conditions of Use

Use of Transeo voice equipment is intended for business use. Individuals must not use Transeo's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual’s own expense using alternative means of communications

Individuals must not:

- Use Transeo's voice facilities for conducting private business.

- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

Actions upon Termination of Contract

All Transeo equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Transeo at termination of contract.

All Transeo data or intellectual property (including but not limited to sales data, contact lists, and databases) developed or gained during the period of employment remains the property of Transeo and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on Transeo computers, servers, or vendors is the property of Transeo. There is no expectation of individual data privacy when using Transeo technology services.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Transeo has the right to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

It is your responsibility to report suspected breaches of security policy without delay to your manager. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Transeo disciplinary procedures.

SECURITY

Physical Security

Transeo's SaaS environment meets or exceeds the following security standards:

1. SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
2. SOC 2
3. SOC 3
4. FISMA, DIACAP, and FedRAMP
5. DOD CSM Levels 1-5
6. PCI DSS Level 1
7. ISO 9001 / ISO 27001
8. ITAR
9. FIPS 140-2
10. MTCS Level 3

In addition, our data centers are compliant with FERPA data hosting standards. Transeo utilizes AWS data centers that are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. Automatic fire detection and supression equipment has been installed to reduce risk. The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Data Encryption

All data transmitted to and from Transeo and the district is secured in no less than 256 bit cryptography. Import and export files that are transmitted between the district and the data center will be transferred using HTTPS and SSL technology via SFTP. All data is encrypted at rest and in transit.

User Authentication

User authentication can be configured to use encrypted usernames and passwords stored within the Transeo application. Transeo can also authenticate users with your District's Active Directory, LDAP, Google, or ClassLink service.

Application Security

The Transeo application security model is based upon user roles. Individual access to system functionality can also be restricted from within the application. Auditing and logging is available to review events which occurred in the system.

Security testing occurs during the specification, development, and quality assurance phases of product development. During the specification phase, security concerns are considered and incorporated into the design of new features and bug fixes. During development, standard patterns and practices are used to ensure that the code generated accounts for security. Unit testing, integration testing, and code reviews cover various edge cases.

Content Delivery Network (CDN)

Transeo enhances the software design and delivery method by utilizing a diverse and robust Content Delivery Network. Our global network of caching locations, the on-demand scalability of our IP network and our full suite of CDN services ensures that your user experiences meet their expectations and needs.

DDOS Protection

Transeo utilizes advanced network security protocols through Cloudflare that protect against DDOS attacks. In the event of such an attack, Cloudflare agrees to redirect all traffic through their web servers to reduce the load on Transeo while they determine which traffic is legitimate.

Operating System Security

Transeo monitors all incoming network connections and traffic, logging all network access attempts and authentication requests. All unnecessary access points have been disabled to the hosted environment and internal services have private subnet IP addresses for ingress routes.

Logs

Transeo streams logs from four primary sources: application logs, Kubernetes orchestration logs, Nginx access logs, and AWS ELB logs. These files are compressed and transmitted to AWS S3 via Fluentd and analyzed using Chaossearch. These logs do not contain student PII.

Credential Security

Transeo does not store any sensitive credentials inside of source control repositories. All credentials are handled via environment variables passed into the application container at runtime. These credentials can only be accessed via our Kubernetes orchestration cluster, which few Transeo employees have access to.

Database Security

Transeo encrypts all database data at rest and in transit. Credentials are stored on machines via environment variables and are not available to individual Transeo employees. Primary databases have limited IP whitelists that prevent unauthorized parties attempting logins.

Database Security

Data storage and security is a major concern for all enterprise applications. Given the nature of the customers we serve and the data that we house, we have built a very robust reliability system. Our services are orchestrated by Kubernetes and containerized via Docker, with the entire setup declared using Terraform. This setup allows us to quickly spin up new machines to handle unexpected events, as well as leaning on built-in AWS features for auto-scaling technology.

We perform full database backups daily as well as support point-in-time restoration. Our Kubernetes clusters do not include storage blocks and all logging files are sent to S3 and indexed via Chaossearch.