STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, ILLINOIS, IOWA, MISSOURI, NEBRASKA, NEW HAMPSHIRE, NEW JERSEY, NEW YORK, OHIO, RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA

MA-ME-IL-IA-MO-NE-NH-NJ-NY-OH-RI-TN-VT-VA-DPA, Modified Version 1.0

Suffolk Public Schools

and

Peachjar, Inc.

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Suffolk Public Schools, located at 100 N. Main St, Suffolk, Virginia, 23434 USA (the "**Local Education Agency**" or "**LEA**") and Peachjar, Inc., located at 8697 La Mesa Blvd, Suite C, La Mesa, CA 91942 (the "**Provider**).

WHEREAS, the Provider is providing educational or digital services to LEA.
WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and
WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.
NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   √ If checked, the Supplemental State Terms and attached hereto as **<u>Exhibit "G"</u>** are hereby incorporated by reference into this DPA in their entirety.

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

   √ If Checked, LEA and Provider agree to the additional terms of modifications set forth **<u>in Exhibit "H".</u>**

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 **<u>Exhibit "A"</u>** (the "**Services**").

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

The designated representative for the Provider for this DPA is:

Name: Joe Cremer Title: Director of Product and Engineering

Address: 8697 La Mesa Blvd., Suite C, La Mes, CA 91942

Phone: 858-997-2117 Email: joecremer@peachjar.com

The designated representative for the LEA for this DPA is:

John Littlefield, Director of Technology
100 N. Main St, Suffolk, Virginia, 23434
757-925-6750 johnlittlefield@spsk12.net

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

Suffolk Public Schools

By: Linda Bates
Linda Bates (Jan 21, 2026 10:20:51 EST) Date: 01/21/2026

Printed Name: Linda Bates Title/Position: Coordinator of Purchasing

Peachjar, Inc.

By: Joe Cremer Date: 1/15/2026

Printed Name: Joe Cremer Title/Position: Director of Product and Engineering

<u>STANDARD CLAUSES</u>
Version 3.0

ARTICLE I: PURPOSE AND SCOPE

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

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

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

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

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

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

4. **<u>Law Enforcement Requests</u>**. 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 within sixty days of termination of the DPA. 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,the LEA may make reasonable inquiries of the Provider regarding the use of the LEA's Student Data and the security measures undertaken by the Provider to protect said Student Data.

. 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. 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 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 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

Peachjar, District approved digital flyers from the schools, district, and community organizations are sent to Peachjar for hosting on a "Flyerboard" and for emailing to parents and guardians. Parents and guardians may access and browse approved digital flyers on the Peachjar "Flyerboard".

EXHIBIT “B”

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	x
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	x
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	x
	Student grade level	x
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	x
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

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

Category of Data	Elements	Check if Used by Your System
	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

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

1. Extent of Disposition

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

[**Insert categories of data here**]

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

2. Nature of Disposition

______Disposition shall be by destruction or deletion of data.

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

[**Insert or attach special instructions**]

3. Schedule of Disposition

Data shall be disposed of by the following date:

______As soon as commercially practicable.

______By [**Insert Date**]

4. Signature

____ ____________________

Authorized Representative of LEA Date

5. Verification of Disposition of Data

____ _______________

Authorized Representative of Company Date

<u>EXHIBIT “F”</u>
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

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

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

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

EXHIBIT "G"
Massachusetts

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

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

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

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

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

EXHIBIT "G"
Maine

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

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

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

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
    a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
    b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
    c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT "G"
Illinois

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Illinois. Specifically, those laws are to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205; and

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

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

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

1. Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be replaced with: "This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed."

2. Replace Notices with: "Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid."

3. In Article II, Section 1, add: "Further clarifying, in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest."

4. In Article II, Section 2, replace "forty-five (45)" with "five (5)". Add the following sentence: "In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA."

5. In Article II, Section 4, replace it with the following: "In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure."

6. In Article II, Section 5, add: Upon request, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1)."

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

8. In Article IV, Section 6, replace the whole section with:

   The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

   If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

   Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

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

10. In Article IV, Section 7, add "renting," after "using."

11. In Article V, Section 1 Data Storage: Illinois requires all Student Data to be stored within the United States, Canada, United Kingdom and/or the European Union.

12. In Article V, Section 4, add the following: "'Security Breach' does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure."

13. In Article V, Section 4(1) add the following:

    vi. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and

    vii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

14. In Article V, Section 4, add a section (6) which states:

    In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

    a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;

    b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;

    c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

    as a result of the security breach; and

    d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

15. Replace Article VII, Section 1 with: "In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate."

16. In Exhibit C, add to the definition of Student Data, the following: "Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school

student records", “student temporary record” or “student permanent record” as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) “records” as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) “personal information” as defined in Section 530/5 of PIPA.”

17. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: “The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first.”

18. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

19. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider’s products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.

20. **Student and Parent Access.** Access by students or parents/guardians to the Provider’s programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.

21. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

22. The Provider will not collect social security numbers.

EXHIBIT "G"
Iowa

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Iowa. Specifically, those laws are Iowa Code §§ 22; Iowa Code §§ 715C, 281 I.A.C. 12.3(4); 41; and

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

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

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

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

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

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

4. In Exhibit "C" add to the definition of "Student Data" significant information on progress and growth, experiences, interests, aptitudes, attitudes, abilities, part-time employment, and future plans.

EXHIBIT "G"
Missouri

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

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

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

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

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

EXHIBIT "G"
Nebraska

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Nebraska. Specifically, those laws are Neb. Rev. Stat. Secs. 79-2,104; 79-2,153 to 79-2,155; 79-2, 539; 87-801 to 87-808; and 92 NAC 6; and

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

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

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

1. In Article II, Section 5, add, "Specifically, any written agreement with a Subprocessor will: (1) prohibit the Subprocessor from using Student Data any purpose other than providing the contracted service to or on behalf of the Provider; (2) prohibit the Subprocessor from disclosing any Student Data provided by the Provider with subsequent third parties; (3) and requires the Subprocessor to implement and maintain reasonable security procedures and practices."
2. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
3. In Article IV, Section 4, replace: "Provider will not Sell Student Data to any third party" with "Provider will not Sell or rent Student Data to any third party.
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Nebraska does not require data to be stored within the United States.

EXHIBIT "G"
New Jersey

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Jersey. Specifically, those laws are N.J. Stat. § 56:8-166.4 et seq.; N.J. Stat. § 18A:36-19; N.J. Stat. § 18A:36-19a; N.J. Stat. § 18A:36-35; N.J. Admin Code § 6A:16-7.9; N.J. Admin. Code § 6A:32-2.1; N.J. Admin. Code § 6A:32-7 et. seq.; and

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

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

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. The Provider will not disclose on its web site any personally identifiable information about a student, including, but not limited to student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.
4. The Provider will not process Student Data in violation of State and federal laws that prohibit unlawful discrimination.
5. The Provider will not conduct processing that presents a heightened risk of harm to students without conducting and documenting a data protection assessment of each of its processing activities that involve Student Data.
6. In Article V, Section 1 Data Storage: New Jersey does not require data to be stored within the United States.
7. Add to the definition in Exhibit "C" of Student Data: "The location and times of class trips."

EXHIBIT "G"
Ohio

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

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

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

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

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

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

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

EXHIBIT "G"
Rhode Island

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

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

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

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:

    i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:

    1. The credit reporting agencies
    2. Remediation service providers
    3. The attorney general

    ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

    iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT "G"
Tennessee

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

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

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

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

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

EXHIBIT "G"
Vermont

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

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

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

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

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

EXHIBIT "G"
Virginia

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

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

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

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

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

EXHIBIT "G"
New Hampshire

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

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

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

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

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

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

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

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

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

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,…"
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

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

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

    (2) Limit unsuccessful logon attempts;

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

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

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

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

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

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

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

    (10) Perform maintenance on organizational systems;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.

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

EXHIBIT "I" – TEACHER DATA

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

Exhibit "G"

New York

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

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

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

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

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

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

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

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

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

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

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

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

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

10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying that it and it's subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any assurance of discontinuation, which will control in the case of a conflict.

    Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D",** or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **"Exhibit D".**

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

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

13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

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

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

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

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

    i. The name and contact information of the reporting LEA subject to this section.

    ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

    iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

    iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

    v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

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

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

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

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

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

    (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals, .

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

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

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

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

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

16. To add to Exhibit "C" the following definitions:
    - **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
    - **APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
    - **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
    - **Disclose or Disclosure**: The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
    - **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
    - **Release:** Shall have the same meaning as Disclose
    - **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
    - **Participating School District**: As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

    -

Exhibit "J"

LEA Documents

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

Exhibit "K"
Provider Security Policy

Provider's Data Security and Privacy Plan attached

Exhibit "K" - Peachjar Information Security Policy.pdf

Peachjar, Inc. Information Security Policy

12/21/2023

Version 1

Table of Contents

Introduction

Overview

Peachjar, Inc. ("Company") is committed to maintaining the integrity and security of confidential or proprietary information of the Company and its customers ("Company Information") and customer non-public information and it is the commitment of the Company to secure that information from unauthorized use. Company embodies this commitment in specific, required policies and security procedures, as collectively set forth in this Information Security Policy ("Policy"). Compliance with this Policy is mandatory for all employees of Company ("Employees") and outside contractors ("Third Party Non-Employees") granted access to Company's networks, servers, systems, computers, software, and information (collectively "Systems").

All Employees and Third Party Non-Employees are expected to familiarize themselves with this Policy.

The purpose of this Policy is to ensure that the Company has taken steps to ensure the availability, confidentiality and integrity of Company Information. Company has identified potential sources of vulnerability of Company Information (defined herein), such as:

- Unauthorized incursion by third parties into Company information maintained electronically on servers and other databases or on paper.
- Unauthorized interception of Company information in transit from one secure Company location to another, or between a secure Company location and an external location.
- Unauthorized access to Company information by Employees or Third Party Non-Employees.
- Unauthorized changes, additions, deletions, misdirection or distribution of Company Information.
- Unauthorized interference with the availability of Company information needed for Company-authorized purposes; and
- Misuse of Company information.

The nature of the precautions required to reduce those risks will vary based on the sensitivity of Company Information and the architecture of the systems on which that information is stored. Nevertheless, the objective in each instance should be to prevent the unauthorized disclosure, change or interruption to Company Information.

Scope

This Policy applies to all Company Information, whether in paper, stored voice or electronic form, and to anyone who has access to Company information or to the Systems. This Policy is mandatory for all Employees and Third Party Non-Employees granted access to Company systems.

Exceptions to this Policy may be requested on a case-by-case basis by contacting the Director of Engineering or Head of Human Resources.

Organization, Ownership and Enforcement

The Director of Engineering is the owner of this Policy and responsible for its approval. The Director of Engineering in conjunction with the Company's Chief Executive Officer ("CEO") or the Company's Chief Financial Officer ("CFO") must approve any deviations from this Policy.

If an Employee violates any of the terms of this Policy, the Employee may be subject to disciplinary actions, including but not limited to, oral or written warnings, suspension or immediate termination. Company does not promise, imply or represent that one form of disciplinary action will occur before another. If a Third Party Non-Employee violates any of the terms of this Policy, the Third Party Non-Employees contract with Company may be subject to immediate termination for cause, in accordance with its terms. In addition, certain violations of this Policy may result in criminal prosecution and/or liability.

Maintenance of this Policy

This Policy is maintained by the Director of Engineering to ensure relevance, quality and completeness.

Requests for change are reported to the Director of Engineering, which is responsible for analyzing the impact of the change from a trend, business, security and financial perspective. Changes approved by the Director of Engineering will be sent to the CEO and CFO for review prior to implementation.

Company reserves the right to supplement, change or discontinue any portion of this Policy from time to time at its sole discretion.

Review of this Policy

The Director of Engineering, the CEO and the CFO will review the Policy at least annually.

Security Management

Policy Framework

The Company Information Security Policy Framework describes the hierarchical structure of the Policy on information security.

Your Responsibilities

You have a responsibility to maintain and preserve the security of Company information resident on or accessible from Systems to which you have access. You must respect, maintain, and enforce at all times existing Company safeguards against unauthorized access to, or unauthorized use or alteration of Company information.

Management Responsibility

Human Resources and/or IT at Company is responsible for distributing this Policy to Company's Employees and Third Party Non-Employees.

Risk Management

IT risk management must align with the direction provided by the executive management and is performed in accordance with the IT Risk Management Framework.

Business Uses Only

Employees and Third Party Non-Employees may access Company information only for legitimate business purposes and to perform the job functions they have been assigned.

Awareness and Training

All Employees with access to Company information or the Systems must receive and acknowledge a copy of this Policy.

Employees will receive a copy upon hire by the Company. Company shall train all Employees upon hire and at least annually.

Email and Communications Activities

Unless approved by an Employee's manager, Company email will not be automatically forwarded to an external destination.

Physical Security

Protection of Non-Electronic Information

Employees and Third Party Non-Employees are expected to follow the policies set forth in this document in their approach to protection of Company information in non-electronic form (e.g., paper).

Operations Management

Protection of Electronically and Voice-Stored Information

Those Employees and Third Party Non-Employees responsible for designing, implementing or managing Systems, must comply with Company policies for the protection of electronically stored information. Several types of measures are required for protection of Company information stored electronically, whether on servers, individual computers, voicemail systems or other media. These measures include password protection, electronic measures (such as file protection or encryption) and common-sense procedures to minimize the possibility of theft or unauthorized access, change or interruption.

Only Approved Software and Antivirus-Scanned Files May Be Used

As with any computer system, and despite precautions, viruses pose a threat to Company’s Systems. Before any software can be installed or used on any System, the software must be virus-tested and approved for use by the Company IT department.

Configuration Management

All PCs, laptops and workstations should be secured in accordance with Company Policy.

Monitoring

Employees shall have no expectation of privacy in anything they store, send or receive on the Company's network or internet connections.

Authorized individuals within Company may monitor at any time without notice various equipment, devices, systems, and network traffic, as well as inspecting log reports of System access, internet usage, search engine usage, file transfer usage, accessing stored voice-mail messages, retrieving email, documents, and inspecting any other System files. All data created on, transmitted to, received or printed from, stored or recorded on mobile devices for Company business or on behalf of Company is the property of Company regardless of who owns the device. The Company from time to time, will have access to personal data and may be required to turn Employee personal data over to third parties as part of litigation, government investigation, subpoena or for formal discovery. No right of privacy of Employees exists with respect to any information on any System, or any activity conducted through a System. Additionally, Company utilizes additional tools and protective measures to provide internet filtering for items deemed harmful, offensive or otherwise against Company policies. Company has the capability and reserves the right to review, audit, intercept, access and disclose all messages or materials created, received or sent over the electronic communications systems for any purpose. The contents of any computer file, e-mail message, voice mail message or internet use properly obtained for legitimate business purposes, may be disclosed without the permission of the Employee.

Communications Management

Protection of Information in Transit

Company information must not be transmitted between Employees, between Company and Third Party Non-Employees, or between Third Party Non-Employees, except as set forth herein:

Any such transfer must be in accordance with applicable privacy and data protection laws and Company's privacy practices and policies. Questions regarding the requirements of such laws or regulations should be directed to the CEO or CFO.

Sensitive Company Information that is transmitted in electronic form outside of a secure Company environment must be protected using methods as determined by the Company Director of Engineering and in accordance with any applicable policies and guidelines[1] separately developed by the Company. Any customer information received by Company or a Third Party Non-Employee over the internet must be received through a secure method of transmission (e.g., encrypted transmission) and stored in accordance with applicable policies and guidelines separately promulgated by Company.

If Company information is faxed to third parties, the sender should ensure that a “confidential” notation appears on the front page of the fax and take due care to ensure that the fax number is correct and that the fax is expected at that number by the recipient. Faxes containing Company information should not be sent to recipients in the care of third-party kiosks or similar “fax-for-fee” locations, unless necessary due to extraordinary circumstances.

Email and Texting

The Company provides many of its Employees with computer equipment, which may include an internet connection and access to an electronic communications system, to enable them to perform their jobs successfully. Company email addresses should not be used for personal correspondence or mailing lists. Additionally, carbon or forwarding to any Employee’s personal email address of any Company emails containing Personal Information, business information, or any sensitive information is prohibited.

Use of the Email System

The email and texting systems are intended for official Company business. The use of the electronic mail systems may not be used to solicit for commercial ventures, religious or political causes, or outside organizations. In addition, the electronic mail systems may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials.

Emails/Texts Are Not Private

Email and text messages sent using Company communications equipment are the property of Company. As covered above, Employees should not expect that any

[1] Peachjar’s Confidentiality Notice: “This email and any attachments are for the exclusive and confidential use of the intended recipient. If you are not the intended recipient, please do not read, distribute or take action in reliance upon this message. If you have received this in error, please notify us immediately by return email and promptly delete this message and its attachments from your computer system.”

message sent using Company equipment – including those considered to be, or labeled as, personal – will be private.

Email/Text Rules

All Company policies apply to the use of Company's email, texting, chat, and other communications systems (e.g., Slack, Huddle, Zoom, WebEx, JoinMe, GoToMeeting, Skype, Google Meet, Microsoft Teams, Skype, etc. (as applicable)). This means, for example, that an Employee may not use the Company's communications systems to send harassing or discriminatory messages, including messages with explicit sexual content or pornographic images, to send threatening messages, or to solicit others to purchase items for non-Company purposes.

We expect Employees to exercise discretion in using electronic communications equipment. Make sure that messages are professional and appropriate in tone and content. Remember, although email or texts may seem like a private conversation, they can be printed, saved, and forwarded to unintended recipients.

Company email/texts are used for business communications. Slogans or signatures that promote political, religious, or other ideals, or contain "humor" that could offend a customer, vendor, or teammate, cannot be used on Company email.

Access Control

Passwords and Other Keys

All passwords, pass codes, access control devices, keys, security passes/badges and personal identification numbers (collectively, "Credentials") issued for the purpose of accessing Company premises or Systems are the property of the Company. You are not permitted to use any Credentials to access, store or retrieve any Company information unless (i) specifically authorized in a particular instance or (ii) authorized in advance as to the type of Company information and Credentials to be used. Without regard to whether information on any System such as email, voice mail or document files are Credential-protected, you may not access any information on any System maintained by any other Employee unless specifically authorized by the Employee maintaining that information or an Employee with supervisory authority over the Employee maintaining that information. For example, logging onto a System using another Employee's or former Employee's or contractor's user name or Credentials is strictly prohibited.

Passwords and Accounts Security

Passwords must be kept secure and account credentials not shared without prior written approval from the Department of Engineering or other relevant department head. Login passwords and other account credentials regarding Company systems and software must not be shared with non-Employee family and other household members when work is being done at home or other remote setting. Authorized users are responsible for the security of their passwords and accounts. Passwords, passcodes, etc., must never be stored in plain text (i.e., readable) in a file that is in the System. If a hacker gets access to the files, those passwords will be usable by the hacker.

Third Party Access to Company Systems and Information

Third Parties

From time to time, Company may provide or permit access to Company Systems or Company Information to third parties. Third-party service providers should be evaluated for their data security measures and potential data exposure risk prior to having access to Company information, and periodically thereafter. Third-party service providers should be under a written agreement with the Company under which they are required to implement and maintain appropriate security measures for maintaining the confidentiality and security of Company Information.

Acceptable and Unacceptable Activities

Company is firmly committed to providing equal opportunity in all aspects of employment and will not tolerate any illegal discrimination or harassment of any kind. The examples of activities listed below are, in general, prohibited and are also subject to the guidelines for illegal discrimination or harassment as outlined in the current Company Employee Handbook. Employees may be exempted from certain of these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Unacceptable Activities

The following is a non-exhaustive list of activities that are prohibited:

- Using peer-to-peer file sharing or online file storage applications (e.g., Bit Torrent, Box.com, Dropbox, etc.), unless specifically approved by the CFO with notification given to the Director of Engineering. Such approval will only be given for specific use for a defined period of time. Blanket approval for use of peer-to-peer file sharing will not be allowed.
- Activities which are illegal under local, state, federal or international law while utilizing Company-owned resources. Exporting any software, technical information, encryption software or technology out of the U.S. in violation of international or regional export control laws, is illegal. The IT or legal department should be consulted prior to export of any material that is in question.
- Giving out personal information about another person, including home address, personal email address and phone number.
- Creating a user account for a social media or other website or service in another person's name without that person's express permission.
- Any use of Company systems for commercial (regardless whether for profit or nonprofit), or for political statement or lobbying purposes unrelated to or unapproved by Company.
- Excessive use of the Company's network or bandwidth (whether on premises or remotely accessed) for personal business.
- Intentionally seeking information on, obtaining copies of, or modify files, other data, or passwords or security questions and answers belonging to other users, or misrepresenting other users on the Systems.
- Circumventing user authentication or security of any host, network or account unless it is a part of normal job duties.
- Using the Systems to access, download, view, transmit, share or process pornographic material, inappropriate text files (as determined by the system administrator or building administrator), or files dangerous to the integrity of the Systems is prohibited.
- Using in emails or social media posts profanity, obscenity, racist terms, or other language that may be offensive to another user is prohibited. The same is applicable to forwarding emails you may receive that contain such language.
- Streaming non-work related audio or video (e.g., Pandora, Spotify, YouTube, etc.) can substantially reduce the network bandwidth and the network speed for everyone and is prohibited. Certain streaming sites may be blocked per IT policy. If you need access to a blocked site for a legitimate purpose, please contact IT.
- Playing games using Company computers or mobile devices, unless specifically authorized for instructional purposes.
- Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner,

except that duplication and/or distribution of materials for educational or other “fair use” purposes is permitted when such duplication and/or distribution would fall within the fair use doctrine of the United States Copyright Law (Title 17, USC). If you have any questions on what might constitute fair use, contact the IT or legal departments. For example, copying or downloading copyrighted cartoons or comic strips and incorporating them into a presentation or brochure, or posting it on a social media website is likely copyright infringement and the owner could well require you or Company to pay a royalty for its use, even though you may think it is a “fair” non-commercial use of the material.

- Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or the right of privacy or publicity or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Company.
- Establishing network or internet connections to live communications, including voice and/or video (relay chat) for non-work related communications, unless specifically authorized by the system administrator; however, use of internet communications, e.g., Zoom, WebEx, JoinMe, GoToMeeting, Skype, Google Meet, Slack Huddle, Microsoft Teams, etc., is permitted for work-related purposes, but only pursuant to Company policy.
- Destroying, modifying, deleting or abusing in any way Company hardware or software.
- Maliciously using the network to disrupt the use of the network by others or to develop programs that harass other users or infiltrating a computer or computing system and/or damaging or disabling or interfering with the software components of a computer or computing system.
- Sending or forwarding hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors.
- The unauthorized installation of any software, including commercial and non-commercial software, shareware, freeware entertainment software, and all other forms of software and files on Company computers.
- Port scanning or security scanning.
- Executing any form of network monitoring which will intercept data not intended for the Employee's host is prohibited, unless this activity is a part of the Employee's normal job/duty.
- Interfering with or denying service to any user other than the Employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the internet/intranet/extranet.

Computer Software

The Company does not condone the illegal duplication of software. The copyright law is clear. The copyright holder is given certain exclusive rights, including the rights to make and distribute copies. Title 17 of the U.S. Codes states that "it is illegal to make or distribute copies of copyrighted material without authorization." One exception is the users' right to make a backup copy for archival purposes. Unauthorized duplication of software is a federal crime. Penalties include substantial fines and jail terms. For this reason, the following rules apply related to software:

- With regard to use on local area networks or on multiple machines, use the software only in accordance with the software publisher's license agreement.
- An Employee should notify their supervisor/manager, IT department, or the legal department immediately if any misuse of software or related documentation within the Company is suspected.
- Use of unauthorized copies of computer software for either business or personal use will be subject to corrective action, up to or including termination.
- Use of USB flash drives, external hard drives, or other removable media is strictly prohibited unless required for performance of specific job responsibilities, in which case prior written approval is required from the Director of Engineering on a case-by-case basis.
- Software managed on Company-owned or leased computers, tablets, or mobile devices may not be removed without prior authorization from the Director of Engineering All external software installed on cloud infrastructure must be approved in advance by the Director of Engineering.
- On personally-owned devices that are approved to connect to Company's network, users should be cautious about installing software. Take care to only install software from approved, official sources such as Google Play Store on Android devices or the AppStore on Apple devices and only if the software is necessary.
- Employees will not attempt to bypass, alter or remove any of the security software installed on the computing devices, whether those devices are Company-owned or personally-owned. Employees unable to troubleshoot issues should contact the IT department for investigation whenever software is not behaving appropriately.

Personal Use of Company Internet Bandwidth

Streaming non-work related audio or video (e.g., Pandora, Spotify, YouTube, etc.) on the Company network can substantially reduce the network bandwidth and the network speed for everyone and should therefore be limited and must not interfere with responsibilities to be performed. Company has the right to block access at any time to such streaming sites. Certain streaming sites may be blocked per IT policy. If you need access to a blocked site for a legitimate purpose, please contact IT. Employees must not attempt to access files on or areas of the Company's servers to which the Employee does not have a right to access, and any attempt at such access may result in Employee disciplinary action, up to and including termination of employment.

Password Policy and Construction Guidelines

All Employees and personnel that have access to Company computer systems (which includes networks, onsite or remote) must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

This policy applies to any and all personnel who have any form of computer account requiring a password on the organizational network including but not limited to a domain account and email account. It is imperative that there are individual accounts assigned to all personnel with their unique passwords. On NO account can a username and/or password be shared with more than one individual.

- Never write passwords down.
- Never send a password through email.
- Never include a password in a non-encrypted stored document.
- Never tell anyone your password.
- Never reveal your password over the telephone.
- Never hint at the format of your password.
- Never reveal or hint at your password on a form on the internet.
- Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
- Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://.
- Report any suspicion of your password being broken to your IT service desk.
- If anyone asks for your password, refer them to your IT service desk.
- Don't use common acronyms as part of your password.

- Don't use common words or reverse spelling of words in part of your password.
- Don't use names of people or places as part of your password.
- Don't use part of your login name in your password.
- Don't use parts of numbers easily remembered such as phone numbers, social security numbers, dates, or street addresses.
- Be careful about letting someone see you type your password.

The IT department must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password which an attacker with the old password could guess. The following password requirements will be set by the IT security department:

- Minimum Length: 10 characters
- Minimum complexity: No dictionary words included
- Passwords should include a minimum of one each of the four types of characters:
    - Lowercase
    - Uppercase
    - Numbers
    - Special characters such as !@#$%^&*(){}[]
- Password history: Last 10 Passwords.
- Maximum password age: 60 days
- Minimum password age: 1 day
- Account lockout threshold: 5 failed login attempts
- Account lockout duration: 30 minutes.
- Don't store passwords using reversible encryption.
- Password protected screen savers should be enabled and should protect the computer within 30 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer". Or "Win +L"
- Applications must authenticate individual user and not a group. Must not store password in clear text or easily reversible format. Application must not pass the password in clear text over the network and should have some kind of role management such that one user can take over the functions of another without having to know the other's password.

- All Administrator and Network active components passwords to be changed on a quarterly basis.
- The company will see to it that wherever possible to implement Multi-Factor Authentication (MFA) in order to make the access even more secure.
- All Accounts which are not logged in for last 60 days to be locked down automatically for inactivity.

Compliance Measurement

The IT Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the management. Scan for accounts which are not logged in for the last 60 days and to seek a valid justification for the same.

Any exception to this policy must be approved by the IT Department in advance. And any non-compliance an Employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Remove Access Policy

Overview and Purpose

As a predominantly remote organization, allowing users to access Company network resources remotely is critical for productivity. The purpose of this policy is to define standards for connecting to Company's network from any host. These standards are designed to minimize the potential exposure to Company from damages which may result from unauthorized use of Company resources. Damages include the loss of sensitive or Company confidential data, intellectual property, damage to public image, damage to critical Company internal systems, etc.

Scope

This policy applies to all Company Employees, contractors, vendors and agents with a Company-owned or personally-owned computer or workstation used to connect to the Company network. This policy applies to remote access connections used to do work on behalf of the Company.

Remote access implementations that are covered by this policy include, but are not limited to, DSL, VPN, and SSH.

Policy

It is the responsibility of Company Employees, contractors, vendors and agents with remote access privileges to Company's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Company.

Requirements

- Secure remote access must be strictly controlled. Control will be enforced via multi-factor authentication, or public/private keys with strong pass-phrases for, e.g., VPN access. For information on creating a strong pass-phrase see the Password Policy above.
- At no time should any Company Employee provide their login or email password to anyone, not even family members.
- Company Employees and contractors with remote access privileges must ensure that their Company-owned or personal computer or workstation, which is remotely connected to Company's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Company Employees and contractors with remote access privileges to Company's corporate network must not use non-Company email accounts (e.g., personal Gmail, Yahoo, etc.), or other external resources to conduct Company business, so as to ensure that official business is never confused with personal business.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- Non-standard hardware configurations must be approved by the Director of Engineering.
- All hosts (including personal computers) that are connected to Company internal networks via remote access technologies must use up-to-date anti-virus software.
- Personal equipment that is used to connect to Company's networks must meet the requirements of Company-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard remote access solutions to the Company network must obtain prior approval from the Director of Engineering.
- Two-factor authentication must be used to access Company's network remotely. Remote access capabilities must be configured to limit access to only those assets and functions the Director of Engineering approves. You may only use Company-provided means for remote access (for example, VPN

connections, dial-up modems, Company portal, etc.). Do not install or setup any other remote connections, including remote desktop software, without the authorization of the Director of Engineering.

Policy Compliance

Compliance Measurement

The Director of Engineering will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback.

Exceptions

Any exception to this policy must be approved by the Director of Engineering in advance.

Bring Your Own Device (BYOD) Policy

Overview and Purpose

Company Employees and contractors may wish to use their personally-owned mobile devices including (cellphones, smartphones, tablets, laptops and computers) (collectively, **"Personal Devices"**) for work-related purposes. Company allows such access in accordance with this Bring Your Own Device Policy (**"BYOD policy"**).

Scope

This BYOD policy will define the minimum security requirements for BYOD. Employees and contractors who are approved to use their own Personal for access to Company resources will comply with this BYOD policy.

Policy

Eligibility

Only Employees with a legitimate business purpose will be allowed to use their own Personal Devices to access Company systems. The eligibility of a particular Employee will depend on several factors, including but not limited to the Employee's responsibilities, specific role within the organization, geographic location, and the type of an Employee-owned mobile device, including various services and applications available for that device. It is within Company's sole discretion to determine whether an Employee is eligible to use his or her Personal Device for business reasons.

Confidentiality and Proprietary Rights

Company Employees must exercise caution to protect the confidentiality of all Company information accessed through a Personal Device. Company's confidential information and intellectual property, including customer information, Employee information, and trade secrets are all extremely valuable and we are taking great care that such information not be compromised.

All eligible Employees under this BYOD Policy promise to treat such information with the confidentiality and care that the Company expects. Your use of your Personal Device must not jeopardize such information. Guarding against the disclosure of such information is governed by this BYOD Policy and Company's other policies on the confidential nature of its information and that of its customers and other business partners. In addition to strictly following this BYOD Policy, it is critical to exercise common sense and sound judgment to prevent the accidental loss of sensitive, confidential information. Content you create on, or transmit to or from, your Personal Device, and information related thereto, for or on behalf of Company or related to Company's business ("Business") is the property of Company.

Although Company normally has no interest in Employees' personal communications and content, Employees who use their Personal Devices for Company's business purposes should understand that such personal content communications are at-risk in the event of a breach of security. At any time during or after employment, an Employee shall make a Personal Device available for inspection, including the copying of any Company-related information, and Company has the right to monitor Business-related use of the Personal Device. In the event of the need for such inspection and/or copying, the Company will take reasonable steps to avoid viewing personal information on the Personal Device.

Security Requirements

Additionally, eligible users must promise that they will use their Personal Devices with the understanding they will do the following:

- Enable (or submit the Personal Device for installation of) Company's security software on the Personal Device and consent to Company's reasonable efforts to audit and manage the Personal Device and secure its data, including providing Company with any necessary passwords (though access to personal, non-business accounts will normally not be requested).

- Comply with Company's device configuration requirements.
- You must also change passwords as required by the Company.
- Keep the Personal Device's operating system and apps which can be accessed for Business-related purposes current with security patches and updates.
- Prohibit access to Business-related communications, files, data, and apps on the Personal Device by your family, friends, unauthorized business associates, etc.
- Not download, transfer, or store work product or sensitive business content directly to your device, for example via e-mail attachments or store such content on servers or locations (e.g., cloud storage providers such as Apple, Google, Dropbox, etc.) other than those approved by Company. You must promptly erase any such information that is inadvertently downloaded to your Personal Device. Any business content on your Personal Device may be accessible to a hacker if your Personal Device or apps are hacked or if you allow access by others.

You must use your best efforts to physically secure your Personal Device against loss, theft, or use by persons who do not have Company's authority to access the content on the Personal Device.

What to Do if Your Personal Device is Lost, Stolen, or Hacked

If your device is lost, stolen, accessed by unauthorized persons (or if such access is suspected), or otherwise compromised, you must immediately notify infosec@peachjar.com to enable Company to protect its confidential business information. Company will assess the damage and, if necessary, remotely erase the Personal Device. Failure to so immediately notify Company in such an event could result in disciplinary action.

Company's Information Technology policies and procedures, including but not limited to its Electronic Communications Systems Policy, apply to all Business uses of your Personal Device. Prior to long-term discontinuance of use of your Personal Device (e.g., if you get a new Personal Device and store, recycle, or trash it) or transfer the Personal Device to someone else, you agree to do a factory reset of the Personal Device.

Departing Employees

Departing Employees must allow Company to remove any Company-related software or controls, and any of Company's work product or sensitive business content from their Personal Devices. Employees who discontinue their use of their Personal Devices must also work with Company to preserve, transfer such content, and to clear their devices of Company's content.

Technological Support

Company does/does not provide technological support for Employee-owned Personal Devices.

Violations of BYOD Policy

Company expects violations of this BYOD Policy to be reported immediately. Employees suspected of or determined to have violated this BYOD Policy will be subject to discipline, up to and including termination of employment.

Compliance with Laws

This BYOD Policy is not intended to restrict communications or actions protected or required by state or federal law. Also, you agree to use your Personal Device in accordance with applicable laws and regulations (e.g., no texting while driving; hands-free use requirements; etc.).

Termination of Employment

Upon resignation or termination of employment, all Company data on personal devices must be removed upon termination of employment. At any time on request, the Employee or contractor may be asked to produce the personal device for inspection.

Violations of Policy

Employees who have not received authorization in advance from the Director of Engineering will not be permitted to use personal devices for work purposes. Failure to follow Company policies and procedures may result in disciplinary action, up to and including termination of employment.

Policy Compliance

Compliance Measurement

The Director of Engineering will verify compliance to this BYOD policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback.

Exceptions

Any exception to this BYOD policy must be approved by the Director of Engineering in advance.

Clean Desk Policy

Overview

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an Employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase Employee's awareness about protecting sensitive information.

Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our Employees, our intellectual property, our customers and our vendors is secure in locked areas.

Scope

This policy applies to all Employees, whether in the office or in their remote workspace, and visiting Third Party Non-Employees.

Policy

- Employees are required to ensure that all Company Information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

- Computer workstations must be locked when the workspace is unoccupied.
- Computer workstations should be restarted at the end of the work day.
- Any Company Information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Company Information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Company Information must not be left at an unattended desk.
- Laptops, tablets and permissible external drives must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on notes posted on, under or near a computer or the work area, nor may they be left written down in an accessible location.
- Printouts containing Company Information should be immediately removed from network/shared printers.
- Company Information documents to be disposed of should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Company Information should be erased immediately after use.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CD-ROM, DVD, and USB drives as sensitive and secure them in a locked drawer.
- All shared printers and fax machines should be cleared of papers as soon as they are printed. This helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Personal Data Storage Policy

Storing personal data or software, including but not limited to photographs, videos, music files, etc. on Company's local or network storage devices is prohibited.

Any personal data or software stored on the Company's network or local storage devices is not backed up and may be deleted immediately and without notice to the account owner.

Data Security Incident Internal Notification Policy

The Company may have legal obligations to report, mitigate, or otherwise respond to any loss or inadvertent disclosure of confidential or protected information related to the Company, its work, its customers, or its personnel. Personal information such as Social Security, credit card, or account numbers can be used for identity theft. The potential of unauthorized access to the Company's data or technologies is considered a security incident. Common examples of such incidents include, but are not limited to, loss or theft of technology devices, unlocked mobile technology left unattended, a notification of a virus or malware infection, and improperly managed login information. A security incident does not mean an actual security breach has occurred; only that one was possible due to the incident. Reporting an incident as soon as identified is an important measure in minimizing a potential security breach by allowing proper security mitigation steps and communications to occur. Any user made aware of an unreported security incident is required to notify the Director of Engineering immediately, day or night.

It is critical that any response to a breach be timely, consistent, and appropriate under the circumstances.

Accordingly, in the event of any (i) actual or potential loss of hard copy documents or an electronic "device" (such as a computer, laptop, tablet, smartphone, flash drive, or other data storage device) containing or potentially containing confidential or protected information, or (ii) the inadvertent disclosure of confidential or protected information (e.g., wrongly directed email or suspicion of hacking on your device):

- If your device may be affected:
  - Do not shut down or reboot your device.
  - Immediately disconnect the remote session by removing the Ethernet cable (not the power cable) from the back of the computer if you are connected by remote to the network, but do not shut down or log off, or, disconnect from the Wi-Fi network.
  - Do not delete anything. Do not try to fix whatever symptoms are occurring.
- Immediately orally advise the Company's Director of Engineering. Do not send emails or leave detailed phone messages about the incident. Do not delay reporting in the hope that the documents or device might be located later.
- Document what happened. Document any information you know including date, time, and the nature of the incident (e.g., what you did just prior to noticing something wrong, or if you inadvertently clicked on an email or attachment you suspect may be bad). Any information you can provide will aid in responding in an appropriate manner. Preservation of evidence is critical.
- Do not discuss the situation with anyone else, including the customer or potentially affected individuals, or take any other action to attempt to resolve the issue, unless directed to do so by the Company's Engineering Director.
- Follow further direction from the Company's Engineering Director.

Peachjar_SuffolkCounty_VA_clean_final_signed

Final Audit Report 2026-01-21

Created:	2026-01-21
By:	TEC SDPA (mmcgrath@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAP0ylzyloJaafvkrh10slUX4j-sjU8q4I

"Peachjar_SuffolkCounty_VA_clean_final_signed" History

Document created by TEC SDPA (mmcgrath@tec-coop.org)

2026-01-21 - 3:18:45 PM GMT

Document emailed to Linda Bates (lindabates@spsk12.net) for signature

2026-01-21 - 3:18:57 PM GMT

Email viewed by Linda Bates (lindabates@spsk12.net)

2026-01-21 - 3:19:58 PM GMT

Document e-signed by Linda Bates (lindabates@spsk12.net)

Signature Date: 2026-01-21 - 3:20:51 PM GMT - Time Source: server

Agreement completed.

2026-01-21 - 3:20:51 PM GMT

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: ~~[LEA],~~Suffolk Public Schools, located at ~~[LEA Address]~~100 N. Main St, Suffolk, Virginia, 23434 USA (the “**Local Education Agency**” or “**LEA**”) and ~~[Provider],~~ Peachjar, Inc., located at ~~[Provider Address]~~ 8697 La Mesa Blvd, Suite C, La Mesa, CA 91942 (the “**Provider**~~”).~~).

WHEREAS, the Provider is providing educational or digital services to LEA.
WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and
WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.
NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   ~~√~~√ If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.

   ~~√~~√ If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

   √ If Checked, LEA and Provider agree to the additional terms of modifications set forth **in Exhibit "H".**

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.

~~6.~~5. 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.

~~7.~~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.~~within sixty days of termination of the DPA. 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.

~~8.~~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~~ may make reasonable inquiries of the Provider ~~will allow~~ regarding the use of the ~~LEA to audit~~ LEA's Student Data and the security ~~and privacy~~ measures ~~that are in place to ensure protection of Student Data or any portion thereof as it pertains to~~undertaken by the ~~delivery of services to the LEA~~Provider to protect said Student Data.

. 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. 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 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.

~~(5)~~(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

~~(6)~~(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 the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms~~ will control~~. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

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

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

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

7. ~~–~~**Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of~~ all or~~

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.

~~4.~~5.In Article II, Section 4, replace it with the following: "In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure."

~~5.~~6.In Article II, Section 5, add: ~~"By no later than (5) business days after the date of execution of the DPA~~Upon request, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1)."

~~6.~~7.In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."

8. In Article IV, Section 6, replace the whole section with:

> The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.
>
> If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.
>
> Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

~~10.~~9. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

~~11.~~10. In Article IV, Section 7, add "renting," after "using."

~~12.~~11. In Article V, Section 1 Data Storage: Illinois requires all Student Data to be stored within the United States, Canada, United Kingdom and/or the European Union.

~~13.~~12. In Article V, Section 4, add the following: "'Security Breach' does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure."

~~14.~~13. In Article V, Section 4(1) add the following:

vi. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and

vii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

~~15.~~14. In Article V, Section 4, add a section (6) which states:

In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;

b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;

c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA-

as a result of the security breach; and

~~c.~~d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

~~16.~~15. Replace Article VII, Section 1 with: "In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate."

~~17.~~16. In Exhibit C, add to the definition of Student Data, the following: "Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school

~~defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school~~ student records", “student temporary record” or “student permanent record” as that term is~~-~~
defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) “records” as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) “personal information” as defined in Section 530/5 of PIPA.”

~~18.~~17. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: “The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first.”

~~19.~~18. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

~~20.~~19. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider’s products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.

~~21.~~20. **Student and Parent Access.** Access by students or parents/guardians to the Provider’s programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.

~~22.~~21. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

~~23.~~22. The Provider will not collect social security numbers.

EXHIBIT "G"
Vermont

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

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

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

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

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

~~4.~~1.~~In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."~~

~~5.~~1.~~All employees of the Provider who will have direct contact with students shall pass criminal background checks.~~

~~6.~~3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT "G"
Virginia

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

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

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

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

~~7.~~1.~~In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."~~

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

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

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

~~2.~~4. In Article V, Section 4, add: In order to ensure the LEA's ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

Exhibit "G"
New York

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

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

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

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

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

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

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

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

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

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D",** or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **"Exhibit D".**

~~0.~~ To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after ~~10.~~11. (iii) account holder, "which term shall not include students."

~~11.~~12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

~~12.~~13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's ~~facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.~~
facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

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

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

~~13.~~14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part
121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

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

i. The name and contact information of the reporting LEA subject to this section.

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

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

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

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

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

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

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals, .

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

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

~~14.~~15. To amend the definitions in Exhibit "C" as follows:

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