SCHEDULE E
EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and What's the MOOV, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to personally identifiable: student data, student demographics, scheduling, attendance, grades, health and discipline tracking. Protected Data also includes all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts that ESBOCES and/or the participating school district has identified to Contractor in writing as sensitive or confidential data of ESBOCES and/or the participating school district. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of ESBOCES and/or participating school districts 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy provided to Contractor in advance of executing this Agreement. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall delete all of ESBOCES' and/or participating school districts' Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option, or direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, ESBOCES or the institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

What's the MOOV, Inc.

DocuSigned by:

BY: Kevin Camson
E0E2EDABF4FE428...

DATED: 11/13/2023

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

MOOV Data Security and Privacy Plan

New York Education law §2-d(5)(e)

Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy.

1. MOOV complies with its responsibilities under all applicable state and federal laws and regulations that protect the confidentiality of personally identifiable information and Student Data

The protection of the privacy and confidentiality of Student Data is tremendously important to MOOV. Student Data means any information (in any format) that is directly related to any identifiable current or former student that is maintained by MOOV for, or on behalf of, its customers.

MOOV complies with its responsibilities under all applicable state and federal laws and regulations that protect the confidentiality of personally identifiable information and Student Data, including the Federal Family Educational Rights and Privacy Act ("**FERPA**"), 20 U.S.C.§ 1232(g); Children's Online Privacy Protection Act ("**COPPA**"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("**PPRA**"), 20 U.S.C. 1232; and applicable State laws governing the protection of personally identifiable information from students' educational records, including New York Educational Law Section 2-d and Part 121 of the Commissioner's Regulations. In particular, MOOV:

- Limits internal access to education records to those individuals that are determined to have legitimate educational interests
- Does not use education records for any other purposes than those explicitly authorized in contracts
- Except for authorized representatives and subcontractors, does not disclose any personally identifiable information to any other party without the consent of the parent or eligible student or unless required by statute or court order and the educational agency has been given notice of the disclosure
- Maintains reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in our custody
- Does not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose and will not facilitate the use or disclosure of Personally Identifiable Information (PII) by any other party for marketing or commercial purposes.

When MOOV contracts with an educational agency, district or BOCES in the State of New York, MOOV agrees to comply with the data security and privacy policy of the agency, district of BOCES and the Parents Bill of Rights for Data Privacy and Security, which is incorporated into the agreement between MOOV and the agency, district or BOCES. For the purposes of compliance with the laws and regulations of New York, "Student Data" also means "student data" and "teacher or principal data" as such terms are defined by New York Education Law 2-d.

2. MOOV implements administrative, operational and technical safeguards and practices to protect the confidentiality and security of PII and Student Data

Administrative:

MOOV limits access to PII only to team members who have a legitimate need to access such data, in order to perform their job functions. For team members, agents and contractors who will access or process Student Data, MOOV provides team member training on privacy and data security laws and best practices on a yearly basis and has implemented disciplinary processes for violations of our information security or privacy requirements. Upon termination or applicable role change, we promptly remove data access rights and/or require the return or destruction of data.

Additionally, MOOV conducts an annual security audit.

Technical:

MOOV has adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework. Additionally, MOOV uses encryption technology to protect student information while in transit and at rest. While in transit, MOOV uses TLS with strong ciphers, with a preference for those with perfect-forward secrecy. While at rest, MOOV uses modern cryptographic algorithms (AES256-GCM) and follows key management best practices, with strict user access control to keys. This ensures that the PII requires a particular key to decrypt and encrypt. Additionally, the controls to access and modify these keys are kept secure.

MOOV's infrastructure runs on Google Cloud Platform (GCP), an industry leader in cloud services and data security. GCP, and other cloud services, have experience in: running and securing servers in the cloud for many customers, navigating and managing security standards, as well as investment in network and physical security. Ernst & Young LLP performs the GCP System and Organization Controls audit and has a publicly available report on how they meet these compliance controls and objects at https://cloud.google.com/security/compliance/soc-2.

MOOV employs physical security controls, such as access controls to secure environments and virtual access controls including role-based authentication and strong password policies. MOOV also utilizes secure development lifecycle practices, having security protocols inform every aspect of product and infrastructure development. This includes threat modeling and code review for major changes, separation of development and production environments, automated log collection and audit trails for production systems, and policies and procedures for network and operations management. MOOV performs annual vulnerability assessments and cloud infrastructure audits.

MOOV also maintains a business continuity program, with data backup and recovery capability that is designed to provide a timely restoration of MOOV services with minimal data loss in the event of a catastrophic failure or disaster.

3. MOOV has implemented team member training on privacy and security obligations.
MOOV yearly provides team member training on privacy and data security laws and best practices on both the federal and state level. Additionally, we train new team members as a part of onboarding. Access to sensitive data systems is gated upon completion of privacy and security training.

4. MOOV oversight of, and responsibility for, sub-contractors
MOOV limits access to PII only to those team members or trusted service providers who have a legitimate need to access such data in the performance of their duties or in connection with providing services to MOOV or on MOOV's behalf. MOOV requires subcontractors to be contractually bound to uphold the same standards for security, privacy, and compliance as are imposed on MOOV by applicable state and federal laws and contracts. MOOV reviews subcontractor contracts annually. MOOV maintains access log(s) that record all disclosures of or access to PII within its possession and will provide copies of those access log(s) to the District upon request. MOOV will make available a list of all such subcontractors upon request.

5. Security incident response plan
MOOV has an information security incident management protocol to detect, assess, mitigate and respond to security incidents and threats. If MOOV believes that there has been unauthorized acquisition or disclosure that compromises the security, integrity or confidentiality of a customer's personal information, we will take all necessary steps to notify the affected customers of the incident as quickly as possible, and in no case greater than two business days after we learn of the breach. Once the communication has been drafted and finalized, within 72 hours of discovery of the incident in the absence of any statutes or custom agreements, we will use MOOV's standard outgoing email systems to send the email to the address associated with the MOOV district account owner.
To the extent known, this notice will identify (i) the nature of the Security Incident, (ii) the steps we have executed to investigate the Security Incident, (iii) the type of personal information affected, (iv) the cause of the Security Incident, if known, (v) the actions we have taken or will take to remediate any deleterious effects of the Security Incident, and (vi) any corrective actions we have taken or will take to prevent a future Security Incident.
If the incident triggers any third-party notice requirements under applicable laws, MOOV will comply with its notification obligations under applicable law and the terms of its contractual agreement with the customer.

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at: http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, Or, by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   MOOV will only use student data or teacher or principal data for the purposes explicitly authorized in its contract with BOCES - specifically providing and facilitating the use of its products and services (e.g., distributing communications, messages, and other information via the web and mobile apps).

2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

   MOOV limits access to PII only to those team members or trusted service providers who have a legitimate need to access such data in the performance of their duties or in connection with providing services to MOOV or on MOOV's behalf. MOOV requires subcontractors to be contractually bound to uphold the same standards for security, privacy, and compliance as are imposed on MOOV by applicable state and federal laws and contracts. MOOV reviews subcontractor contracts annually. MOOV maintains access log(s) that record all disclosures of or access to PII within its possession and will provide copies of those access log(s) to the District upon request. MOOV will make available a list of all such subcontractors upon request.

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   MOOV destroys all confidential information obtained in connection with the services provided herein and/or student data. Destruction of the confidential information and/or student data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction.

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

   Complaints should be directed to: The Associate Superintendent for Curriculum for your district; Or in writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

   MOOV's infrastructure (including data storage and encryption) runs on Google Cloud Platform (GCP), an industry leader in cloud services and data security. GCP, and other cloud services, have experience in: running and securing servers in the cloud for many customers, navigating and managing security standards, as well as investment in network and physical security. Ernst & Young LLP performs the GCP System and Organization Controls audit and has a publicly available report on how they meet these compliance controls and objects at https://cloud.google.com/security/compliance/soc-2.

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;

7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.