

New York

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: Ontario-Seneca-Yates-Cayuga-Wayne BOCES (the “Local Education Agency” or “LEA” or “New York Original LEA”) and Mosa Mack Science, Inc. (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 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 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;

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

1. Provider agrees to offer the LEA all the same terms and conditions found in the **MA-ME-NH-RI-VT-NDPA, Standard Version 1.0** Data Privacy Agreement between the Provider and **Worcester Public Schools** (“Originating LEA”) which is dated **10/21/22** (“Originating DPA”). The terms and conditions of the Originating DPA are thus incorporated herein.
2. Provider additionally agrees to the following additional terms outlined in the attached Exhibit “G” for New York, which will control in the event of a conflict between the DPA and the Originating DPA.
3. Provider may, by signing the attached form of “General Offer of Privacy Terms” be bound by the terms of the General Offer of Privacy Terms to any other LEA who signs the acceptance on said Offer. The form is limited by the terms and conditions described therein.
4. **Notices.** All notices or other communication required or permitted to be given pursuant to the Originating DPA may be given for the LEA 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: Lissa Johnson Title: CEO
Address: 21 Buena Vista Rd, Fairfield, CT 06825
Phone: 202-253-7610 Email: lissa@mosamack.com

The designated representative for the LEA for this DPA is:

Sue Marcano, Sr. Application Support Services Assistant
sue.marcano@edutech.org
131 Drumlin Ct, Newark, NY 14513

Ontario-Seneca-Yates-Cayuga-Wayne BOCES

By: *Kelli Eckdahl*
Date: 07/15/24
Printed Name: Kelli Eckdahl
Title/Position: Director

Mosa Mack Science, Inc.

By: *Lissa Johnson*
Date: 7/19/2024
Printed Name: Lissa Johnson
Title/Position: CEO

Exhibit "G"

New York

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 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 Contractor 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 costs 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

LEA’s Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy for this service agreement can be accessed at:

<https://go.boarddocs.com/ny/wflboces/Board.nsf/goto?open&id=AR6P6W62FF9F>

<https://docushare.edutech.org/dsweb/Get/Document-588382/WFL%20BOCES%20EduTech%20Parent%20Bill%20of%20Rights%202022.pdf>

Exhibit "K"
Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at:

Included as an attachment

https://mosamack.com/privacy_policy#:~:text=What%20does%20Mosa%20Mack%20do,can%20continually%20improve%20the%20product.

MosaMack._OntarioSeneca_NY_Addition_VendorSigned

Final Audit Report

2024-07-22

Created:	2024-07-20
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAApFIY8APcEaMmcCdXJYuGzmefIDV-M92

"MosaMack._OntarioSeneca_NY_Addition_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-07-20 - 7:56:52 AM GMT
-  Document emailed to Kelli Eckdahl (kelli.eckdahl@edutech.org) for signature
2024-07-20 - 7:56:56 AM GMT
-  Email viewed by Kelli Eckdahl (kelli.eckdahl@edutech.org)
2024-07-22 - 11:25:18 AM GMT
-  Document e-signed by Kelli Eckdahl (kelli.eckdahl@edutech.org)
Signature Date: 2024-07-22 - 11:25:32 AM GMT - Time Source: server
-  Agreement completed.
2024-07-22 - 11:25:32 AM GMT

The designated representative for the Provider for this DPA is:


Name: Lissa Johnson Title: CEO
Address: 21 Buena Vista Rd. Fairfield, CT 06825
Phone: 202/253-7610
Email: info@mosamack.com

The designated representative for the LEA for this DPA is:

Marco Andrade, Ph.D., Director, Office of Research and Accountability
Worcester Public Schools
20 Irving Street, Rm. 202 | Worcester, MA 01609
508-799-3060
andradem@worcesterschools.net

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

WORCESTER PUBLIC SCHOOLS


By: 
[Marco Andrade \(Oct 21, 2022 11:06 EDT\)](#)

Date: 10/21/2022

Printed Name: Marco Andrade

Title/Position: Director of Research and Accountability

MOSA MACK SCIENCE, INC.

By: 

Date: 9/29/2022

Printed Name: Lissa Johnson

Title/Position: CEO