

8/20/2026

DATA PRIVACY AND SECURITY AGREEMENT

WHEREAS, eDynamic, having its offices 1256 Main Street, Suite 256, Southlake, TX 76092 (hereinafter "Contractor") and the Genesee Valley Board of Cooperative Educational Services, 80 Munson Street, LeRoy, New York 14482 (hereinafter "GVB"), collectively "the Parties," are parties to an agreement dated 08/21/2024 (hereinafter the "Master Agreement") through which Contractor will provide eDynamic Learning courseware and

WHEREAS, pursuant to the Master Agreement, Contractor will receive student data and/or teacher or principal data in possession of GVB and/or its officers, employees, agents, and students, and may also receive student data and/or teacher or principal data of educational agencies within New York State that contract with GVB for the use of Contractor's products and/or services; and

WHEREAS, in entering into this Memorandum of Agreement (hereinafter "MOA") the Parties seek to amend the terms of that Master Agreement in conformance with N.Y. Education Law § 2-d and 8 N.Y.C.R.R. § 121.1, *et seq.*

NOW, THEREFORE, the Parties mutually agree that the Master Agreement is hereby amended as follows:

1. For purposes of this MOA, terms shall be defined as follows:
 - a. "Breach" means the unauthorized acquisition, access, use, or disclosure of personally identifiable student data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.
 - b. "Commercial Purpose" or "Marketing Purpose" means the sale of personally identifiable student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of personally identifiable student data for advertising purposes, or to develop, improve or market products or services to students.
 - c. "Disclose" or "Disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.
 - d. "Education Records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
 - e. "Eligible Student" means a student who is eighteen years or older.
 - f. "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United

States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

- g. "Parent" means a parent, legal guardian, or person in parental relation to a student.
 - h. "Personally Identifiable Information," as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in N.Y. Education Law §3012-c (10).
 - i. "Release" shall have the same meaning as Disclosure or Disclose.
 - j. "Student" means any person attending or seeking to enroll in an educational agency.
 - k. "Student data" means personally identifiable information from the student records of an educational agency. For purposes of this agreement, "student data" includes information made accessible to Contractor by GVB, GVB officers, GVB employees, GVB agents, GVB students, and/or the officers, employees, agents, and/or students of educational agencies with whom GVB contracts.
 - l. "Teacher or principal data" means 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 N.Y. Education Law §§ 3012-c and 3012-d. For purposes of this agreement, "teacher or principal data" includes information made accessible to Contractor by GVB, GVB officers, GVB employees, GVB agents, GVB students, and/or the officers, employees, agents, and/or students of educational agencies with whom GVB contracts.
 - m. "Unauthorized Disclosure" or "Unauthorized Release" means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.
2. Contractor agrees that the security, confidentiality, and integrity of student data and/or teacher or principal data shall be maintained in accordance with:
- a. Applicable state and federal laws that protect the confidentiality of personally identifiable information;
 - b. The terms and conditions of this MOA, including but not limited to the GVB Parents Bill of Rights for Data Security and Privacy and the Supplemental Information to Parents Bill or Rights for Data Privacy and Security, attached hereto

as Exhibit A; and

c. Applicable GVB policies, which can be accessed on the GVB website at: <http://www.gvboces.org/policies.cfm>.

3. Contractor will not use subcontractors in fulfilling its responsibilities to GVB, its employees or agents, and/or educational agencies which contract with GVB for the provision of Contractor's products and/or services, and Contractor will endeavor to apply standards of protecting personally identifiable student information in a manner no less stringent than Contractor's policy in protecting personally identifiable information. *[IF CONTRACTOR WILL USE SUBCONTRACTORS, SPECIFY HOW THEY WILL MANAGE THOSE RELATIONSHIPS TO ENSURE PROTECTION OF PII]*

The eDynamic Holdings LP will provide the district with educational records including PII required to administer student progress in eDynamic Learning courses in the Learning Management System (Agilix Buzz).

eDynamic will ensure that subcontractors or others that the company shares PII with will abide by data protection and security requirements of district policy, and state and federal law and regulations by implementing, regularly reviewing and enforcing contractual obligations with subcontractors. Those contractual obligations include but not limited to:

- A. Limitations on data use and disclosure (PII cannot be sold; access to PII is limited to system administrators and can only be used to provide the service; PII cannot be disclosed outside of specific exceptions outlined in FERPA)
- B. Specific administrative controls that contractors must have in place that are consistent with eDynamic Learning administrative control policies (privacy training, background checks, password policies, breach notification obligations)
- C. Data retention policy that accommodates right to be forgotten
- D. Data security and encryption requirements

4. Contractor agrees that it will disclose student data and/or teacher or principal data only to those officers, employees, agents, subcontractors, and/or assignees who need access to provide the contracted services. Contractor further agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to that data. *[SPECIFY HOW SUCH TRAINING WILL BE PROVIDED, AND HOW THE THIRD-PARTY CONTRACTOR WILL ENSURE THOSE INDIVIDUALS WILL ABIDE BY DATA SECURITY AND PROTECTION REQUIREMENTS]*.

eDynamic provides regular scheduled privacy and security training to employees that have access to student personally identifiable information (PII), it also has contractual obligations with subcontractors to provide training to subcontractor employees (minimum on yearly basis). The subcontractors also are obligated to have administrative controls in place such as background checks and internal policies to protect student data.

5. The exclusive purpose for which Contractor is being provided access to personally identifiable information is providing and administering courses in the Learning Management System. The information is only used for Legitimate Educational Purposes and is covered by School official exception of The Family Educational Rights and Privacy Act (FERPA).

6. Student data and/or teacher or principal data received by Contractor, or by any subcontractor or assignee of Contractor, shall not be sold or used for marketing purposes.

7. The agreement between Contractor and GVB for eDynamic Learning courseware 08/21/2024 expires on 08/20/2026. Upon expiration of that agreement without a successor agreement in place, and upon ninety (90) days' written notice, Contractor shall assist GVB and any educational agencies that contracts with GVB for the provision of Contractor's products or services in exporting any and all student data and/or teacher or principal data previously received by Contractor back to GVB or the educational agency that generated the student data and/or principal data. Contractor shall, upon ninety (90) days' written notice, securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the extraction, transmission, deletion, or destruction of student data and/or teacher or principal data will be completed within 90 days of receiving written notice from BOCES to Contractor, and will be accomplished utilizing an approved method of confidential deletion or destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. To the extent that Contractor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Contractor and/or its subcontractors or assignees will provide a certification to GVB from an appropriate officer that the requirements of this paragraph have been satisfied in full.

8. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by GVB or the educational agency that generated the student data for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the applicable educational agency's Annual Professional Performance Review Plan.

9. Student data and/or teacher or principal data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility located in the United States, or a data facility maintained by a Board of Cooperative Educational Services. In order to protect the privacy and security of student data and/or teacher or principal data stored

in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures shall include, but are not necessarily be limited to disk encryption, file encryption, firewalls, and password protection. *[PROVIDE ADDITIONAL, SPECIFIC INFORMATION REGARDING THE ADMINISTRATIVE, OPERATIONAL, AND TECHNICAL SAFEGUARDS CONTRACTOR HAS IN PLACE TO PROTECT THE PII IT RECEIVES]*

Password protections include:

- a. Internal administrative password policies
- b. Two-actor authentication for AWS access for admins
- c. Optional Single Sign on features available to district users to authenticate students and teachers (SAML or CAS)
- d. Ability for district users to configure various minimal password policies for district users

Administrative procedures include:

- a. Regular contract reviews
- b. Scheduled Security reviews
- c. Background checks on employees
- d. Privacy training for employees that have access to customer PII

Encryption while PII is in motion and at rest:

- a. We employ various encryption protocols to ensure data is encrypted in motion and at rest. This includes but not limited to: SL/TLS, AES256, encrypted storage volumes for encryption at rest254.

Firewalls: Various types of network protection mechanism including:

- a. DMZ Networks/ Firewalls;
- b. Load balancers,
- c. Network restricted access to databases

Other:

- a. Managed Detection and Response Service (MDR), to reduce likelihood and reduce impact of cybersecurity attacks
- b. Web applications include input validation, output encoding and other OWASP top best practices to protect against vulnerabilities

10. Contractor acknowledges that it has the following obligations with respect to any student data and/or teacher or principal data provided pursuant to its agreement with GVB, and any failure to fulfill one of these obligations set forth in New York State Education Law § 2-d and/or 8 N.Y.C.R.R. Part 121 shall also constitute a breach of its agreement with GVB:

- a. Limit internal access to education records to those individuals that are determined to have legitimate educational reasons within the meaning of § 2-d and the Family Educational Rights and Privacy Act;

- b. Not use education records/and or student data for any purpose other than those explicitly authorized in this Agreement;
- c. Not disclose any personally identifiable information to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under this Agreement, unless (i) that other party has the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- d. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody;
- e. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);
- f. Notify GVB of any breach of security resulting in an unauthorized release of student data by Contractor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but not more than seven (7) calendar days after discovery of the breach;
- g. Where a breach or unauthorized release of personally identifiable information is attributable to Contractor, Contractor will pay or reimburse GVB and/or any educational agencies which contract with GVB for the provision of Contractor's products or services for the cost of any notifications GVB and/or such other educational agencies is/are required to make by applicable law, rule, or regulation; and
- h. Contractor will cooperate with GVB and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

11. In the event of a data security and privacy incident (including but not limited to a breach, unauthorized release, and/or unauthorized disclosure) implicating the personally identifiable information of students, teachers, and/or principals of GVB or educational agencies which contract with GVB for the provision of Contractor's products or services, Contractor will:

- a. *[INCLUDE MEASURES TAKEN TO IDENTIFY BREACHES AND UNAUTHORIZED DISCLOSURES]* eDynamic and its subcontractors has a variety of measures in place to identify breaches and unauthorized access including but not limited to AWS audit trails, Managed Detection and Response Service

(MDR), to reduce likelihood and reduce impact of cybersecurity attacks and access log reviews;

b. Notify GVB in accordance with Education Law § 2-d, 8 N.Y.C.R.R. Part 121, and paragraph 10(f), above.

12. Contractor, its employees and representatives shall at all times comply with all applicable federal, state, and local laws, rules, and regulations.

13. This MOA, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, constitutes the entire understanding of the Parties with respect to the subject matter thereof. The terms of this MOA, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, shall supersede any conflicting provisions of Contractor's terms of service or privacy policy.


14. If any provision of this MOA shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court finds that any provision to this MOA is invalid or unenforceable, but that by limiting such provision it would become valid or enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

15. This MOA shall be binding on any successors of the parties. Neither party shall have the right to assign its interests in the MOA to any other party, unless the prior written consent of the other party is obtained.

16. This MOA shall be governed by the laws of the State of New York. Any action or proceeding arising out of this contract shall brought in the appropriate courts of New York State.

In witness of the foregoing, the duly authorized representatives of the Parties have signed this Memorandum on the date indicated.

FOR THE Genesee Valley BOCES:



[NAME] Jon Sanfratello
[TITLE] Director of Programs

6/11/24
Date

FOR THE CONTRACTOR:

E-SIGNED by Brian Piccioni
on 2024-06-12 15:59:01 GMT

Brian Piccioni
Chief Financial Officer

June 12, 2024
Date

EXHIBIT A: PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Genesee Valley BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the district, to enhance the opportunities for learning and to increase the efficiency of our operations. To assist in meeting legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law, Genesee Valley BOCES has posted this Parents Bill of Rights for Data Privacy and Security.

- 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. The procedures for exercising this right can be found in Student Records Policy, No. 6420.
- 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 at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
- 5) Parents have the right to have complaints about possible breaches of student data addressed.
 - a. Parents may make a written report of a possible breach of student data to the Genesee Valley BOCES Data Protection Officer, 80 Munson Street, LeRoy, NY 14482 or by phone 585-658-7900.
 - b. Complaints may also be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234 or by submitting a form at:
<http://www.nysed.gov/data-privacysecurity/report-improper-disclosure>
- 6) To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
- 7) Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
- 8) Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Supplemental Information to Parents Bill of Rights for Data Privacy and Security:

1. The exclusive purpose for which Contractor is being provided access to student data and/or teacher or principal data is access, administration and support of eDynamic courses. All student data access is provided for legitimate educational interests only, as defined in FERPA. Student data and/or teacher or principal data received by Contractor, or by any assignee of Contractor, from GVB or its employees, officers, agents, and/or students will not be sold or used for marketing purposes.

Student data and/or teacher or principal data received by Contractor, or by any assignee of Contractor, from GVB or its employees, officers, agents, and/or students will not be sold or used for marketing purposes.

2. Contractor agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data. More specifically, *[ADD INFORMATION REGARDING HOW THE THIRD-PARTY CONTRACTOR WILL ENSURING TRAINING, AND OTHER MEASURES TAKEN TO ENSURE SUBCONTRACTORS OR ASSIGNEES ABIDE BY DATA PROTECTION AND SECURITY REQUIREMENTS]*

eDynamic will ensure that subcontractors or others that the company shares PII with will abide by data protection and security requirements of district policy, and state and federal law and regulations by implementing, regularly reviewing and enforcing contractual obligations with subcontractors. Those contractual obligations include but not limited to:

- a. Limitations on data use and disclosure (PII cannot be sold; access to PII is limited to system administrators and can only be used to provide the service; PII cannot be disclosed outside of specific exceptions outlined in FERPA)
- b. Specific administrative controls that contractors must have in place that are consistent with eDynamic Learning administrative control policies (privacy training, background checks, password policies, breach notification obligations).
- c. Data retention policy that accommodates right to be forgotten.
- d. Data security and encryption requirements.

3. The agreement between Contractor and GVB for eDynamic Learning courseware expires on 08/20/2026. Upon expiration of that agreement without a successor agreement in place, and upon ninety (90) days' written notice, Contractor will assist GVB in exporting any and all student data and/or teacher or principal data previously received by Contractor back to GVB. Contractor will, upon ninety (90) days' written notice, securely delete any and all student data and/or teacher or principal data remaining in its possession or the possession of its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data), as well as any and all student data and/or teacher or principal data maintained on its behalf of in secure data center facilities. Contractor will ensure that no copy, summary, or extract of the student data and/or teacher or principal data, or any related work papers, are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned

secure data center facilities. Any and all measures related to the extraction, transmission, deletion, or destruction of student data and/or teacher or principal data will be completed within ninety (90) days written notice from BOCES to Contractor. To the extent that Contractor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they/it will not attempt to re-identify de-identified data and will not transfer de-identified data to any party.

4. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the GVB for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the BOCES Annual Professional Performance Review Plan.

5. Student data and/or teacher or principal data transferred to Contractor by GVB or GVB officers, employees, agents, or students will be stored in electronic format on systems maintained by Contractor in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry standards and the NIST Cybersecurity Framework Version 1.1. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection. *[IF POSSIBLE, PROVIDE ADDITIONAL, SPECIFIC INFORMATION REGARDING THE MEASURES CONTRACTOR WILL TAKE TO PROTECT PII]*

Password protections include:

- Internal administrative password policies
- Two-actor authentication for AWS access for admins
- Optional Single Sign on features available to district users to authenticate students and teachers (SAML or CAS)
- Ability for district users to configure various minimal password policies for district users

Administrative procedures include:

- Regular contract reviews
- Scheduled Security reviews
- Background checks on employees
- Privacy training for employees that have access to customer PII

Encryption while PII is in motion and at rest:

- We employ various encryption protocols to ensure data is encrypted in motion and at rest. This includes but not limited to: SL/TLS, AES256, encrypted storage volumes for encryption at rest254.

Firewalls: Various types of network protection mechanism including:

- DMZ Networks/ Firewalls;

- Load balancers,
- Network restricted access to databases

Other:

- Managed Detection and Response Service (MDR), to reduce likelihood and reduce impact of cybersecurity attacks
- Web applications include input validation, output encoding and other OWASP top best practices to protect against vulnerabilities

6. Any student data and/or teacher or principal data possessed by Contractor will be protected using encryption while in motion and at rest.

7. Acknowledged and agreed to by:

Signature: E-SIGNED by Brian Piccioni
on 2024-06-12 15:59:03 GMT
Brian Piccioni

Name: Brian Piccioni

Title: Chief Financial Officer

Date: June 12, 2024