

Appendix B

Compliance With New York State Education Law Section 2-d Contract Addendum ("Addendum")

The parties to this Contract Addendum are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and n2y LLC ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d"), and Vendor is a third party contractor, as that term is used in Section 2-d. BOCES and Vendor have entered into this Contract Addendum to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of this Contract Addendum, the terms of this Contract Addendum shall apply and be given effect.

Definitions

As used in this Addendum and related documents, the following terms shall have the following meanings:

"Student Data" means personally identifiable information from student records that Vendor receives in connection with providing Services under this Agreement.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student 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.

"BOCES" means Monroe #1 Board of Cooperative Educational Services.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student" means any person attending or seeking to enroll in an educational agency.

"Eligible Student" means a student eighteen years or older.

"State-protected Data" means Student Data, as applicable to Vendor's product/service.

"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.

"Breach" means the unauthorized access, use, or disclosure of personally identifiable information or Educational Agency Data.

"Commercial or marketing purpose" means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students.

"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement;

(c) not disclose any personally identifiable information to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained 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 the personally identifiable information in its custody;

(e) use encryption technology to protect data while in motion or in its custody from unauthorized disclosure by 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 using a technology or methodology specified by the secretary of the U.S.);

(f) 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;

(g) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor 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 no more than seven (7) calendar days after such discovery of such breach;

(h) cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, and that comply with the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the Data belongs to and is owned by the Participating School District from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may otherwise be applicable to its customers or users of its product/service, to the extent

that any term of such online terms of service or Privacy Policy conflicts with the terms of this Addendum or the Agreement, the terms of this Contract Addendum first and then the Agreement (with Exhibits) shall be given precedence; and

(k) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full cost of such breach notification to parents and eligible students due to the unauthorized release of student data by Vendor or its agent or assignee.

Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security

<https://www.monroe.edu/domain/1478>

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all 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.

To further these goals, the 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 6320. (<https://www.monroe.edu/6320>)
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/documentalioin/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. Complaints should be directed in writing, to:

Chief Privacy Officer
New York State Education Department
Room 863 EBA
89 Washington Avenue
Albany, New York 12234.

or

Monroe One Data Protection Officer
William Gregory
Monroe #1 BOCES
41 O'Connor Road
Fairport, NY 14450

Supplemental Information About Agreement Between n2y and BOCES

- (a) The exclusive purposes for which the personally identifiable information will be used by Vendor is to provide the n2y subscription services to BOCES and/or a Participating School District pursuant to a purchase order
- (b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.
- (c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.
- (d) The effective date of this Addendum shall be from the effective date the Agreement and it shall remain in effect until June 30, 2025, unless terminated sooner or renewed for an additional term. This Agreement shall automatically renew for one (1) year periods following the term, unless terminated by either party at any time and for any reason upon thirty (30) days' notice.
- (e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.
- (f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.
- (g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above.