Exhibit A
Education Law Section 2-d Contract Addendum

The parties to this Contract Addendum (this "Addendum") are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and Arctic Wolf Network Solutions, Inc. ("Vendor" or "Arctic Wolf"). This Addendum is incorporated in the Solutions Agreement dated simultaneously herewith (the "Agreement") to which this Addendum is attached. Any capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement. 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 its implementing regulations, and Vendor is a third party contractor, as that term is used in Section 2-d and its implementing regulations. 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 the Agreement 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 are included in Solutions Data and received by Vendor from an educational agency (including BOCES or a Participating School District) in connection with providing Solutions 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 Solutions.

"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 PII stored within Vendor's systems.

"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 other than as may be expressly authorized by the Agreement (the "Solutions").

"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 included in Solutions Data and received in connection with providing the Solutions 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, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the Solutions);

(b) only use PII 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 PII received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under the Agreement, unless (i) 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 PII in its custody;

(e) use encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering PII 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 or permitted by the secretary of the U S.);

(f) not sell PII received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Solutions, 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, in compliance with New York law and regulation;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of PII by Vendor;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, are no less restrictive than those policies and practices set forth in Vendor's SOC2 Type II in place on the Effective Date, and are in substantial compliance with 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 State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may 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 applicable law or regulation, the terms of the applicable law or regulation shall apply;

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required Breach notification to parents and eligible students due to the unauthorized release of Student Data caused by Vendor or its agent or assignee;

(m) ensure that employees, assignees and agents of Vendor who have access to Student Data receive or will receive training on the federal and state laws governingthe confidentiality and handling of such data prior to receiving access to such data; and

(n) ensure that any subcontractor that performs Vendor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and this Addendum.

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/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. 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 Arctic Wolf Solutions and BOCES

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide the managed detection and response security operations solutions and other product/services described in the Agreement to BOCES or other Participating School District pursuant to a BOCES 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 Contract Addendum shall be April 18, 2023, and the Agreement and Addendum shall remain in effect during the initial term of the Agreement and any renewal term, unless sooner terminated in accordance with the terms of the Agreement.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format set forth in the Agreement. Vendor shall thereafter securely delete all Solutions Data and any any all personally identifiable information included therein 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 such data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the Solutions Data and personally identifiable information contained therein are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance with the terms of this Addendum. 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. 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, substantially aligns with NIST Cybersecurity Framework, Version 1.1, and the practices and policies set forth in Vendor's SOC2 Type II Report, 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. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vender affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as **Attachment 1** and is incorporated herein by reference as if fully set forth herein.

DocuSigned by:
Andrew Hill
Vendor Signature

18
April ___, 2023

DS
DS

Is Data Security and Privacy Plan

As per the Agreement between the undersigned and the School District, this plan must be completed by the Service Provider within 10 days of execution of the Agreement.

1. Exclusive Purposes for Data Use
    a. Please list the exclusive purposes for which the student data [or teacher or principal data] will be used by the service provider include.

Personal information will be used for the delivery of solutions provided in the MDR/MR Solutions Agreement between the parties and according to the "Customer Privacy Notice" made available to all customers in https://arcticwolf.com/terms/privacy-notice-for-customers/

Initial DS

2. Data Accuracy/Correction Practices
    a. Parent [student, eligible student, teacher or principal] may challenge the accuracy of the data by...

Eligible Data Subjects may challenge the accuracy of the data by conforming to the policies of the district regarding data challenges. They should directly contact the District which will contact Arctic Wolf, if the challenge is determined to be appropriate within the policies of the District. Arctic Wolf will respond directly to the District within 30 days. If a data subject reaches out to Arctic Wolf directly and identifies themselves as a constituent of the District, Arctic Wolf will contact the District for instructions and inform the data subject that their request has been forwarded to the District.

Initial DS

3. Subcontractor Oversight Details
    a. This contract has subcontractors: Yes ____X____ No_____
    b. Describe how the contractor will ensure subcontractors abide by data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations:

If Arctic Wolf engages subcontractors or other authorized persons or entities to deliver the solutions under the Agreement, it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation to comply with all applicable data protection, privacy and security requirements required of Vendor under the Agreement.

Initial DS

4. Security Practices
   a. Where is the data stored? (described in such a manner as to protect data security)
      In third party data centers located in the country designated on the ordering document or otherwise provided in the Agreement.

   b. The security protection practices taken to ensure data will be protected include:

Data stored in the platform's cloud storage is protected in accordance with the data security controls outlined in Arctic Wolf's SOC2 Type II Report which is issued by an independent third party audit firm post an external audit on an annual basis. Arctic Wolf has vendor risk management practices that ensure data security and privacy terms are in place to protect the data in its third party cloud platforms.

5. Contract Lifecycle Practices
   a. The agreement expires twelve (12) months beginning on the subscription start date.
   b. When the agreement expires,
      i. How long is the student data [or teacher or principal data] retained?
      No more than one hundred twenty (120) days following expiration or termination of the Agreement.
      ii. How is the student data disposed?
      Arctic Wolf will offer District the ability to export the data on its own, or safely dispose of it on District's behalf.

6. Encryption Practices
   a. Data encryption is applied in accordance with Education Law 2-d 5(f)(5)
      Yes___X___ No_____ Initial DS

7. Training Practices
   a. Annual training on federal and state law governing confidentiality is provided for all officers, employees, or assignees who have access to student [or teacher or principal data]
      Yes___X___ No_____ Initial DS

Arctic Wolf Networks, Inc.

Andrew Hill General Counsel
Print Name and Title

DocuSigned by:
Andrew Hill
Signature of Service Provider

4/18/2023
Date