

ADMINISTRATION

Deborah McBride Heppes
Chief Operating Officer

Kerri B. Stroka
Deputy Superintendent

Mark P. Coleman
Assistant Superintendent
Finance and Management Services



BOARD MEMBERS

Eugenia S. Pavek, President
William M. Boss, Vice-President
Michael Bello
Lawrence E. Berger
Martha Bogart
David Eaton
Edwin A. Estrada

Sharleen Depew
Clerk of the Board

ADDENDUM TO AGREEMENT

Regarding

Data Privacy and Security

In Accordance with Section 2-d of the New York Education Law

Including

Parents' Bill of Rights for Data Security and Privacy

AND

Supplemental Information

This Data Privacy and Security agreement is by and between AgileBlue with its principal place of business located 9000 Sweet Valley Dr., Cleveland, OH 44125 ("Contractor"), and **Orange Ulster Board of Cooperative Educational Services**, with its principal place of business located at 53 Gibson Road, Goshen, NY 10924 ("OU BOCES"). Upon being executed by Contractor's and OU BOCES's authorized representatives, this Addendum shall be deemed to have been in full force and effect for the following school years 2025-2027.

WHEREAS, OU BOCES is an educational agency within the meaning of New York State Education Law, Section 2-d ("Section 2-d"), and Contractor is a third party contractor within the meaning of Section 2-d; and

WHEREAS, Contractor and its authorized officers, employees, students and agents shall have access to "student personally identifiable information (PII)," "student data" and/or "teacher or principal data" regulated by Section 2-d; and

WHEREAS, the provisions of this Addendum are intended to comply with Section 2-d in all respects. To the extent that any term of the Agreement conflicts with the terms of this Addendum, the terms of this Addendum shall apply and be given effect.

NOW, THEREFORE, it is mutually agreed that the Agreement is hereby amended in accordance with this Addendum, as follows:

1. Confidential Information

1.1 Contractor agrees that in performing the Original Agreement with the OU BOCES, Contractor may have access to confidential information in the possession of OU BOCES, including student, teacher or principal personally identifiable information ("PII"). For the purposes of this Addendum and the Original Agreement, it is agreed that the definition of Confidential Information includes all documentary, electronic or oral information made known to Contractor or developed or maintained by Contractor through any activity related to the Original Agreement. This Confidential information includes student, teacher and/or principal data (as the terms are defined under Section 2-d.)

- 1.2 Contractor agrees to comply with Section 2-d, and the corresponding regulations promulgated by the Commissioner of Education of New York (“Commissioner”) thereunder. In addition, Contractor agrees to comply with any changes in Section 2-d, the Commissioner’s regulations and relevant OU BOCES policy that may be amended or modified during the term of the Original Agreement. Upon request by OU BOCES, Contractor shall provide OU BOCES with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor’s own information security policies, confidentiality obligations, and applicable laws.
- 1.3 Upon expiration of the Agreement to which this Addendum applies, without a successor agreement in place, Contractor shall assist OU BOCES in exporting all student, teacher and/or principal data previously received by Contractor from, or developed on behalf of, OU BOCES, and Contractor shall, at the request of OU BOCES, either securely delete any student, teacher and/or principal data remaining in Contractor's possession or return the student, teacher and/or principal data to OU BOCES. If student, teacher and/or principal data is to be maintained by Contractor for any lawful purpose, such data shall remain in an encrypted format and shall be stored on systems maintained by Contractor in a secure data facility located within the United States.
- 1.4 The parties further agree that the terms and conditions set forth in this Confidential Information section and all of its subparts shall survive the expiration and/or termination of the Original Agreement.

2. Data Inspection and Challenges to Data

Education Law Section 2-d and FERPA provide parents and eligible students the right to inspect and review their child's or the eligible student’s PII stored or maintained by OU BOCES. To the extent PII is held by Contractor pursuant to the Original Agreement, Contractor shall respond within thirty (30) calendar days to OU BOCES’ requests for access to PII so OU BOCES can facilitate such review by a parent or eligible student. If a parent or eligible student contacts Contractor directly to review any of the PII held by Contractor pursuant to the Original Agreement, Contractor shall promptly notify OU BOCES and refer the parent or eligible student to OU BOCES.

In the event that a student's parent or an eligible student wishes to challenge the accuracy of student data (pertaining to the particular student) that may include records maintained, stored, transmitted, and/or generated by Contractor pursuant to the Agreement, the challenge will be processed in accordance with the procedures of OU BOCES.

A teacher or principal who wishes to challenge the accuracy of data pertaining to the teacher or principal personally, which is disclosed to Contractor pursuant to the Agreement, shall do so in accordance with the procedures for challenging APPR data, as established by OU BOCES.

3. Training

Contractor represents and warrants that any of its officers, employees, and/or assignees who will have access to student, teacher and/or principal data pursuant to the Original Agreement will receive training on the federal and state laws governing confidentiality of such student, teacher and/or principal data, prior to obtaining initial or any further access to such data.

4. Use/Disclosure of Data

- 4.1 Contractor shall not sell or use for any commercial purpose student, teacher and/or principal data that is received by Contractor pursuant to the Agreement or developed by Contractor to fulfill its responsibilities pursuant to the Agreement.
- 4.2 Contractor shall use the student, teacher and/or principal data, records, or information solely for the exclusive purpose of and limited to that necessary for the Contractor to perform the duties and services required under the Original Agreement. Contractor shall not collect or use educational records of OU BOCES or any student, teacher and/or principal data of OU BOCES for any purpose other than as explicitly authorized in this Addendum or the Original Agreement.
- 4.3 Contractor shall ensure, to the extent that it receives student, teacher and/or principal data pursuant to the Agreement, that it will not share Confidential Information with any additional parties, including an authorized subcontractor or non-employee agent, without prior written consent of OU BOCES. Contractor shall indemnify and hold OU BOCES harmless from the acts and omissions of the Contractor's employees and subcontractors.

5. Contractor's Additional Obligations under Section 2-d and this Addendum

Contractor acknowledges that, with respect to any student, teacher and/or principal data received through its relationship with OU BOCES pursuant to the Agreement it is obliged to maintain a Data Security & Privacy Plan, and fulfill the following obligations:

- execute, comply with and incorporate as Exhibit "A" to this Addendum, as required Section 2-d, the Parents' Bill of Rights for Data Privacy and Security developed by OU BOCES;
- store all data transferred to Contractor pursuant to the Agreement by OU BOCES, in an electronic format on systems maintained by Contractor in a secure data facility located within the United States or hard copies under lock and key;
- limit internal access to student, teacher and/or principal data to Contractor's officers, employees and agents who are determined to need such access to such records or data to perform the services set forth in the Original Agreement;
- not disclose student, teacher and/or principal data to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under the Agreement, unless: (I) the other party has the prior written consent of the applicable student's parent or of the eligible student; or (II) the other party has the prior written consent of the applicable teacher or principal; or (III) the disclosure is required by statute or court order, and notice of the disclosure is provided to OU BOCES no later than five business days before such information is required or disclosed (unless such notice is expressly prohibited by the statute or court order);

- use reasonable administrative, technical and physical safeguards that align with the NIST Cybersecurity Framework and are otherwise consistent with industry standards and best practices, including but not limited to encryption, firewalls and password protection as specified by the Secretary of the United States Department of HHS in any guidance issued under P.L. 111-5, Section 13402(H)(2), to protect the security, confidentiality and integrity of student and/or staff data of OU BOCES while in motion or in custody of Contractor from unauthorized disclosure;
- not mine Confidential Information for any purposes other than those agreed to in writing by the Parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited; notify OU BOCES, in the most expedient way possible and without unreasonable delay, of any breach of security resulting in an unauthorized release of any PII. In addition, Contractor shall take immediate steps to limit and mitigate the damage of such security breach or unauthorized release to the greatest extent practicable, and promptly reimburse OU BOCES for the full cost of any notifications OU BOCES makes as a result of the security breach or unauthorized release. Contractor further acknowledges and understands that Contractor may be subject to civil and criminal penalties in accordance with Section 2-d for violations of Section 2-d and/or this Agreement.
- understand that any breach of the privacy or confidentiality obligations set forth in this Addendum may, at the sole discretion of OU BOCES, result in OU BOCES immediately terminating this Agreement; and
- Familiarize its applicable officers, employees and agents with this Addendum and with the "Parents' Bill of Rights for Data Privacy and Security."

The Contractor acknowledges that failure to fulfill these obligations shall be a breach of the Agreement. Except as specifically amended herein, all of the terms contained in the Original Agreement are hereby ratified and confirmed in all respects, and shall continue to apply with full force and effect.

IN WITNESS WHEREOF, Contractor and OU BOCES execute this Addendum to the Agreement as follows:

Contractor Name: _____
 By: Tony Pietrocola
 Title: President
 Signature: 
 Date: 10/1/2025

OU BOCES
 By: Mark Coleman
 Title: Assistant Superintendent
 Signature: 
 Date: 10/9/25

Exhibit A

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

In accordance with the requirements of Section 2-d of the New York Education Law, Orange-Ulster BOCES (the "OU BOCES") provides the following Parents' Bill of Rights with respect to maintaining the privacy and security of student data:

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;
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. Towards this end, OU BOCES has implemented the following safeguards to protect personally identifiable information about students, which is stored or transferred by OU BOCES, against unauthorized disclosure.
 - All databases that have student information are protected by a secure password and login. Logins are monitored, and passwords are kept up-to-date.
 - All databases that have student information are protected by a secure firewall, and intrusion detection. All data bases that contain student information are encrypted with 256 bit secure socket layer protection.
4. Parents may access a complete list of all student data elements collected by NYSED at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to: Director of Technology, 4 Harriman Drive, Goshen, NY 10924 (845)781-4358; support@ouboces.org.

PLEASE NOTE: Accordingly, this Parents' Bill of Rights is subject to revision and/or supplementation as needed to comply with OU BOCES' obligations under the law.

Additional information is available on the New York State Education Department's website at: https://www.nysed.gov/sites/default/files/programs/data-privacy-security/parents-bill-of-rights_2.pdf

Exhibit B

Supplemental Information

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, OU BOCES is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	AgileBlue
Description of the purpose(s) for which Contractor will receive/access PII	To enable AgileBlue to provide Managed Detection and Response (MDR) and Security Operations Center (SOC) services to the Customer, which includes the necessary collection, storage, and analysis of data via the Elastic SIEM platform.
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input checked="" type="checkbox"/> APPR Data
Contract Term	Contract Start Date <u>10/01/2025</u> Contract End Date <u>06/30/2028</u>
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> ● Securely transfer data to OU BOCES, or a successor contractor at OU BOCES’ option and written discretion, in a format agreed to by the parties. ● Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting OU BOCES. If a correction to data is deemed necessary, OU BOCES will notify Contractor. Contractor

	agrees to facilitate such corrections within 21 days of receiving OU BOCES' written request.
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p style="text-align: center;">Please see below starting with "AgileBlue is ISO27001:2022 certified."</p>
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	
[Printed Name]	Tony Pietrocoda
[Title]	President
Date:	10/1/2025

AgileBlue is ISO27001:2022 certified.

As a part of our certification, we have the following controls in place that address security and privacy risks for our clients data:

- Role based access controls are implemented internally for AgileBlue employees using least privilege principals on our applications and servers responsible for housing client security logs.
- Access reviews are performed quarterly to ensure access necessary into the environment is performed.
- All security logs accessible to our customers are segmented for each customer to ensure our customers can only see their security logs/cases.
- Backups are performed routinely and stored encrypted where access is limited to a few individuals.
- Annual pentests are performed to identify exploitable vulnerabilities and remediation is performed on all findings.
- AgileBlue routinely performs vulnerability scans to identify vulnerabilities in the environment and remediation plans are put in place to address any findings.
- Security logs collected from our customers are not used for any other purpose other than to identify and alert on threats.
- Employees are trained on various topics of security such as social engineering and data security practices.
- Employees are required to read and attest that they have read and understood all internal policies at least annually.