DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Parent's Bill of Rights for Data Privacy and Security
and
Supplemental Information about the General Terms and Conditions Agreement
between
CEWW BOCES aka Champlain Valley Educational Services and Arctic Wolf Networks, Inc.

1. **Purpose**

(a) CVES BOCES (hereinafter "District" or "CVES BOCES") and Arctic Wolf Networks, Inc. (hereinafter "Vendor") are parties to a contract or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal data that is included in the Data (as defined in the Agreement) and is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services to the District (the "Agreement").

(b) This Exhibit supplements the Agreement to which it is attached, to ensure that the Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Agreement between CVES BOCES and Vendor that the District is required by Section 2-d to post on its website. Any capitalized terms not defined herein shall have the meaning set forth in the Agreement.

(c) In consideration of the mutual promises set forth in the Agreement, Vendor agrees that it will comply with all terms set forth in the Agreement and this Exhibit. To the extent that any terms contained in the Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. Definitions

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive in the Data from the District pursuant to the Agreement.

(b) “Teacher or Principal Data” means personally identifiable information, as defined in Section 2-d, that Vendor may receive in the Data from the District pursuant to the Agreement.

(c) “Protected Data” means Student Data and/or Teacher or Principal Data included in the Data, to the extent applicable to the product or service provided to the District by Vendor pursuant to the Agreement.

(d) “NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. Confidentiality of Protected Data

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with applicable federal and state law (including but not limited to Section 2-d) and the terms of the Agreement.

4. Data Security and Privacy Plan

As more fully described herein, throughout the term of the Agreement, Vendor will maintain security practices and processes no less restrictive than those set forth in set forth in Schedule III of Vendor’s Data Processing Addendum (“DPA”) found at (https://arcticwolf.com/wp-content/uploads/2025/10/Product_Data-Processing-Addendum_2025.10-FINAL.pdf) in place as of the Effective Date, and are in substantial compliance with the CVES BOCES Parents’ Bill of Rights and this Data Sharing and Confidentiality Agreement to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor’s Plan for protecting the District’s Protected Data includes, but is not limited to, its agreement to comply with the terms of the District’s Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Agreement are as follows:

(a) Vendor will implement all applicable state, federal, and local data security and privacy requirements as provided in the Agreement, as well as this Data Sharing and Confidentiality Agreement..

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Agreement between CVES BOCES and Arctic Wolf]." Vendor's obligations described within this section include, but are not limited to:

(i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements imposing confidentiality and data protection obligations no less restrictive that those contained in the Agreement., and

(ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data as provided in the Agreement, upon termination, expiration or assignment (to the extent authorized) of the Agreement.

Vendor has provided or will provide training on the confidentiality and handling of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

(d) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures in accordance with the practices and policies set forth in set forth in Vendor's and those set forth in Schedule III of Vendor's DPA. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to the District by contacting Matt Palkovic directly by email at cvesnetadmin@cves.org or by calling 518.561.0100 x3132.

(c) Vendor will cooperate with the District and provide as much information as possible directly to Matt Palkovic or his/her designee about the incident, including but not limited to and to the extent known: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform Matt Palkovic or his/her designee.

6. **Additional Statutory and Regulatory Obligations** [1]

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District in connection with providing Vendor's products to the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Agreement to which this Exhibit is attached.

[1] Nothing in Education Law Section 2-d or Part 121 specifically requires an educational agency to include within its contracts with third-party contractors this list of obligations that are imposed on third-party contractors by the statute and/or its implementing regulations. However, many school districts and other educational agencies have considered it a best practice to include these statutory and regulatory obligations within their third-party contracts.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Agreement, unless:

(i) the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with Section 2-d and Part 121.

(h) To not sell Protected Data 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.

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, or other binding obligations relating to data privacy and security contained in the Agreement and this Exhibit.

(j) To reasonably cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) Subject to the limitations of liability included in the Agreement, pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors..

BY THE VENDOR:

Andrew Hill

Name (Print)

Signed by:

Andrew Hill

F178AB24F7DC46F...

Signature

DS

BS

General Counsel and Chief Legal Officer

Title

12/19/2025

Date

EXHIBIT [_A_] (CONTINUED)

Supplemental Information about the Agreement between

CVES BOCES and Arctic Wolf Networks, Inc. [2]

CVES BOCES has entered into a Master Agreement with Arctic Wolf Networks, Inc., which governs the availability to the District of the following products:

Arctic Wolf's Managed Detection and Response ("MDR") and Jumpstart Retainer

Pursuant to the Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor may receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data"), in addition to the data ("Data") required for the delivery of Vendor's products as defined in the Agreement.

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor may receive Protected Data within the Data from the District is to provide the District with the functionality of the products listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Agreement.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements

[2] Each educational agency, including a school district, is required to publish a "Bill of Rights for Data Security and Privacy" on its website. *See*, Education Law Section 2-d(3)(a) and Part 121.3(a). The Bill of Rights [that is posted on a district's website] must also include "supplemental information" for each contract that the school district enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data [protected by Education Law Section 2-d]. *See*, Education Law Section 2-d(3)(c) and Part 121.3(c).

Nothing in Education Law Section 2-d or Part 121 requires an educational agency to post its third-party contracts on its website *in their entirety*. In addition, nothing in Education Law Section 2-d or Part 121 requires an educational agency to include the "supplemental information" about each contract, within the contract itself.

However, many school districts and other educational agencies have considered it a best practice to include most or all of the required elements of "supplemental information" within each applicable contract, and have complied with the obligation to include the "supplemental information" for each applicable contract with their Bill of Rights, by posting *the text from this page of this Exhibit* from each applicable contract (or a link to this text) on their website in proximity to their Bill of Rights.

acknowledging to comply with obligations no less restrictive than those required of Vendor under the Agreement.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Agreement commenced on November 19, 2025 and expires upon termination or non-renewal by one or both parties.
- Upon expiration of the Agreement without renewal, or upon termination of the Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data in accordance with the terms of the Agreement. If requested by the District, Vendor will assist the District at termination or expiration of the Agreement, to facilitate the return of the District's Data in accordance with its then-current Data return practices and policies.
- In the event the Agreement is assigned to a successor Vendor (to the extent authorized by the
- Agreement), and to the extent possible the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever after termination of the Agreement. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these deletion requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of Protected Data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any raw Data that Vendor receives will be stored on systems maintained by Vendor, in a secure data center facility located within the United States. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework.