EXHIBIT A-8 STATEMENT OF ASSURANCES

1. In connection with the services contemplated by this Request for Bids/Proposals, will you collect, process, manage, store or analyze student personally identifiable information (PII) or confidential teacher or principal data? Check below as appropriate:

   ☐ **Yes**

   ☒ **No**

2. If you answered "Yes" to #1, include with the bid/proposal submission a letter detailing the following:
   - The specific purpose for which the student PII or confidential teacher or principal data will be used.
   - How Contractor will ensure that subcontractors, or others with whom the company shares PII or confidential teacher or principal data, will abide by data protection and security requirements. Describe methods/procedures to safeguard data use by subcontractors.
   - How and where Contractor will store the PII
   - Identify what reasonable measures Contractor will take to ensure the confidentiality of student PII or teacher or principal data. Describe how the following, as applicable, will be implemented:
     - ☐ Password protections
     - ☐ Administrative procedures
     - ☐ Encryption
     - ☐ Firewalls
   - How and when (within what time frame) the Contractor will destroy its records containing student PII or confidential teacher or principal data, once the Contractor has completed its service to the BOCES

3. If you answered "No" to #1, complete and sign the section below:

"I, the undersigned agent, certify that Central Programs Inc. d/b/a Gumdrop Books **(bidder/proposer name), will not collect, process, manage, store or analyze student PII, or confidential teacher or principal data.**

Authorized Agent:

Name: Barton L. Fitzgerald
(Printed)

Title: President/CEO
(Printed)

By: _____
(Signature)

DATA PRIVACY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE
Agreement

1. Purpose

(a) This Data Privacy Agreement (DPA) supplements the agreement between Capital Region BOCES (BOCES) and Central Programs DBA Gumdrop Books (Vendor), to ensure that the Vendor AGREEMENT conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Agreement consists of the terms of this DPA Agreement, a copy of BOCES Parents Bill of Rights for Data Security and Privacy signed by Vendor and the Supplemental Information about the AGREEMENT that is required to be posted on BOCES website.

(b) To the extent that any terms contained within the Vendor AGREEMENT, or any terms contained within any other Agreements attached to and made a part of the Vendor AGREEMENT, conflict with the terms of this DPA, the terms of this DPA will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the Vendor AGREEMENT, to the extent that any term of the TOS conflicts with the terms of this DPA, the terms of this DPA will apply and be given effect.

2. Definitions

Any capitalized term used within this DPA that is also found in the Vendor AGREEMENT will have the same definition as contained within this DPA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the DPA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the Vendor AGREEMENT.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent

applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the AGREEMENT.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the AGREEMENT may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and BOCES policy on data security and privacy. Vendor acknowledges that BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, and has provided the policy to Vendor.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with the BOCES Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by Vendor and is set forth below.

Additional elements of Vendor' Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this DPA, consistent with BOCES data security and privacy policy, Vendor will: [Gumdrop and subcontractors will collect a minimal amount of data to ensure access control and billing purposes only.]

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Vendor AGREEMENT, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Vendor AGREEMENT:

[Gumdrop and subcontractors use private data bases not visible to the cloud and has restricted internal access.]

(c) Vendor will comply with all obligations set forth in BOCES "Supplemental Information about the AGREEMENT" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows:

[The limited data and the protected databases has limited accessors who are fully aware of confidentiality and we will continue to train as the needs arise.]

(e) Vendor [*check one*] __X__ will _____ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Vendor AGREEMENT. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Vendor AGREEMENT, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in BOCES "Supplemental Information about the Vendor AGREEMENT," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the AGREEMENT is terminated or expires, as more fully described in BOCES "Supplemental Information about the AGREEMENT," below.

5. **Additional Statutory and Regulatory Obligations**

collType text here

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the Vendor AGREEMENT and the terms of this Data Privacy Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the Vendor AGREEMENT.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under

the Vendor AGREEMENT, unless:

(i) the parent or eligible student has provided prior written consent; or

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

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in BOCES "Supplemental Information about the Vendor AGREEMENT," below.

(g) Provide notification to BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Privacy Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are 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 or assignees.

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

(a) Vendor shall promptly notify BOCES of any breach or unauthorized release of Protected Data 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 BOCES by contacting the BOCES Data Protection Officer, at dpo@neric.org.

(c) Vendor will cooperate with BOCES and provide as much information as possible directly to the Data Protection Officer (DPO) or designee about the incident, including but not limited to: 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 personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies 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, BOCES, 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 shall not provide this notification to the CPO directly. 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 BOCES, Vendor will promptly inform the Data Protection Officer or designees.

(e) Vendor will consult directly with the Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

BY Vendor:

Signature

CEO

Title

Febuary 19, 2021

Date

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Albany-Schoharie-Schenectady-Saratoga BOCES (BOCES) is committed to protecting the privacy and security of personally identifiable information about students who attend BOCES instructional programs in accordance with applicable law, including New York State Education Law Section 2-d.

To further these goals, BOCES wishes to inform parents of the following:

(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, including any student data maintained by the Capital Region BOCES. This right of inspection of records is consistent with the federal Family Educational Rights and Privacy Act (FERPA). Under the more recently adopted regulations (Education Law §2-d), the rights of inspection are extended to include data, meaning parents have the right to inspect or receive copies of any data in their child's educational record. The New York State Education Department (SED) will develop further policies and procedures related to these rights in the future.

Requests to inspect and review a child's education record should be directed to: Data Protection Officer, dpo@neric.org, 900 Watervliet-Shaker Road, Albany, NY 12205.

(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 for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or 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 may be directed to the NYS Chief Privacy Officer by writing to the New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: CPO@mail.nysed.gov.

BY Vendor:

Signature

CEO

Title

Febuary 19, 2021

Date

SUPPLEMENTAL INFORMATION

ABOUT THE AGREEMENT BETWEEN
Albany-Schoharie-Schenectady-
Saratoga BOCES AND Vendor

BOCES has entered into An Agreement ("AGREEMENT") with Vendor ("Vendor"), which governs the availability to Participating Educational Agencies of the following Product(s):

Pursuant to the AGREEMENT, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used:

Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the AGREEMENT. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the AGREEMENT and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: [*Describe steps the Vendor will take*] GCType text here

Duration of AGREEMENT and Protected Data Upon Expiration:

- The AGREEMENT commences on [*date*] and expires on [*date*]. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors. If requested by a Participating Educational Agency, Vendor will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.
- At BOCES request, Vendor will cooperate with BOCES as necessary in order to transition Protected Data to any successor Vendor prior to deletion.
- Vendor agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these 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 a Participating Educational Agency to Vendor, by contacting the student's district of

residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

BY Vendor:

Signature

CEO

Title

Febuary 19, 2021

Date

Type text here