

# CONTRACT ADDENDUM

## Protection of Personally Identifiable Information

### 1 .Applicability of This Addendum

The Greater Southern Tier B.O.C.E.S. ("DISTRICT") and the American Welding Society ("Vendor") are parties to a Master Agreement (contract) dated 11/4/2023 ("the underlying contract") governing the terms under which DISTRICT accesses, and Vendor provides, products identified in the Master Agreement. DISTRICT's use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying Master Agreement (contract) and any online Terms of Use or Service published by Vendor.

### 2. Definitions

- 2.1 "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from DISTRICT or is created by the Vendor's product or service in the course of being used by DISTRICT.
- 2.2 "Vendor" means the vendor identified above.
- 2.3 "Educational Agency" means a school district, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes DISTRICT.
- 2.4 "DISTRICT" means the Greater Southern Tier B.O.C.E.S.
- 2.5 "Parent" means a parent, legal guardian, or person in parental relation to a Student.
- 2.6 "Student" means any person attending or seeking to enroll in an educational agency.
- 2.7 "Eligible Student" means a student eighteen years or older.
- 2.8 "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.
- 2.9 "This Contract" means the underlying Master Agreement (contract) as modified by this Addendum.

### 3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

### 4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the

confidentiality of Protected Information, and in accordance with the DISTRICT Data Security and Privacy Policy and Parent's Bill of Rights for Data Privacy and Security, which are included in this document.

#### **5. Vendor Employee Training**

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

#### **6. No Use of Protected Information for Commercial or Marketing Purposes**

Vendor warrants that Protected Information received by Vendor from DISTRICT or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

#### **7. Ownership and Location of Protected Information**

- a. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with DISTRICT. Vendor shall acquire no ownership interest in education records or Protected Information.
- b. DISTRICT shall always have access to the DISTRICT's Protected Information ~~through~~ the term of this Contract. DISTRICT shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.
- c. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by DISTRICT or its authorized users or performing any other data analytics other than those required to provide the Product to DISTRICT. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to DISTRICT upon request.
- d. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All help desk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

#### **8. Purpose for Sharing Protected Information**

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to DISTRICT.

## **9. Downstream Protections**

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

## **10. Protected Information and Contract Termination**

- a. The expiration date of this Contract is defined by the underlying Master Agreement (contract).
- b. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by DISTRICT.
- c. Vendor shall thereafter securely delete and overwrite any and all Protected Information 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 of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.
- d. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.
- e. 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 removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.
- f. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to DISTRICT from an appropriate officer that the requirements of this paragraph have been satisfied in full.

## **11. Data Subject Request to Amend Protected Information**

- a. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

- b. Vendor will cooperate with DISTRICT in retrieving and revising Protected Information but shall not be responsible for responding directly to the data subject.

## **12. Vendor Data Security and Privacy Plan**

- a. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the District's Data Security and Privacy Plan as set forth in this addendum .
- b. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:
  - i. align with the NIST Cybersecurity Framework 1.0;
  - ii. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;
  - iii. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the DISTRICT data security and privacy policy as set forth in this addendum.
  - iv. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;
  - v. demonstrate that it complies with the requirements of Section 121.3(c) of this Part; specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access ;
  - vi. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;
  - vii. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify DISTRICT; and
  - viii. describe whether, how and when data will be returned to DISTRICT, transitioned to a successor contractor, at DISTRICT's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

## **13. Additional Vendor Responsibilities**

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any

failure to fulfill one of these statutory obligations shall be a breach of this Contract:

- a. Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;
- b. Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;
- c. Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the DISTRICT unless (i) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to DISTRICT no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- d. Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;
- e. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);
- f. Vendor will notify the DISTRICT of any breach of security resulting in an unauthorized release of student data by the 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 calendar days after the discovery of the breach; and
- g. Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse DISTRICT for the full cost incurred by DISTRICT to send notifications required by Education Law Section 2-d.

**14. The District's Data Security and Privacy Policy, referenced herein, is as follows:**

#### **DATA SECURITY AND PRIVACY POLICY**

The BOCES will comply with and implement the provisions of the Family Educational Rights and Privacy Act (FERPA), Education Law §§ 2-d, 101, 305 and their implementing or related regulations.

In particular, the BOCES will, in complying with and implementing these laws and regulations, take the following actions regarding the personally identifiable information of its students, parents, and staff:

1. The BOCES will not sell such personally identifiable information nor use it or allow it to be used for any marketing or commercial purpose and will minimize the collection, processing, and transmission of such information.
  - a. The BOCES will ensure that it has provisions in its contracts with third party contractors that require that the confidentiality of such personally identifiable information be maintained.
  - b. The BOCES shall not report to NYSED juvenile delinquency, criminal, or medical and health records, or biometric information of its students, except as required by law.
2. The BOCES will publish on its website a parents' bill of rights for data privacy and security which is attached to this policy and that complies with the requirements of 8 NYCRR Part 121.
  - a. This parents' bill of rights will include certain provisions regarding such personally identifiable information that each third party contract must contain, include the purpose that any such personally identifiable information will be used, how subcontractors will abide by all data security and privacy requirements, the duration of the contract, how a parent, student or staff member may challenge the accuracy of any such personally identifiable data that is used, where such personally identifiable information will be stored and the precautions taken to protect such information, and how the information will be encrypted while it is in motion.
  - b. Such provisions will be published on the BOCES' website and may be redacted in accordance with the law and regulations.
3. Procedures for individuals to file complaints about breaches or unauthorized releases of such personally identifiable information will be established and communicated.
  - a. As part of these procedures, the BOCES will acknowledge receipt of complaints, commence and investigation, and take necessary precautions to protect such personally identifiable information.
  - b. The BOCES will provide the complainant with its findings within 60 days from the receipt of the complaint.
  - c. The BOCES will maintain a record of all such complaints.
4. The BOCES adopts the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Cyber Security Framework or NIST CSF) as its standard for data security and privacy.

5. Every use and disclosure of such personally identifiable information by the BOCES shall benefit students and the BOCES. Such personally identifiable information shall not be included in public reports or other documents.
6. A copy of this policy shall be published on the BOCES' website and all notice of the policy will be provided to all BOCES' officers and employees.
7. Each third-party contract entered into by the BOCES shall include the third-party contractor's data security and privacy plan, which shall:
  - a. Outline how the third-party contractor will comply with state, federal, and local data privacy and security laws, regulations, and policies regarding protection of such personally identifiable information.
  - b. Specify the safeguards and practices that the contractor has in place to protect such personally identifiable information.
  - c. Specify how training on the federal and state laws regarding privacy of such personally identifiable information will occur.
  - d. Specify how subcontractors will be managed to ensure such personally identifiable information will be protected.
  - e. Specify how incidents involving breaches or unauthorized disclosures of such personally identifiable information will be identified and managed, and how the BOCES will be notified in the event of such breach or disclosure.
  - f. Specify how data will be returned to the BOCES or deleted or destroyed at the termination or expiration of the contract.
8. The BOCES shall annually provide data security awareness training to their officers and employees with access to such personally identifiable information in accordance with 8 NYCRR Part 121.
9. The BOCES shall designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law § 2-d and 8 NYCRR Part 121, and to serve as the point of contact for data security and privacy of the BOCES.
10. The BOCES shall ensure that all third-party contractors shall be in compliance with the requirements of 8 NYCRR 121.9.
11. Breaches and unauthorized releases of such personally identifiable information.
  - a. Third-party contractors shall promptly notify the BOCES of any breach or unauthorized release of such personally identifiable information.





- d. A complete list of all student data elements collected by New York State is available for public review at the following website <http://www.nysed.gov/student-data-privacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
- e. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Data Privacy Officer, Computer Services Center, GST BOCES, 459 Philo Road, Elmira, NY 14903.

**16. The Vendor agrees to protect the protected information of the students, teachers, and principals of GST BOCES by addressing the following issues in the following manner:**

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, are as follows:

Student and instructor data will be used to align students to the correct instructors and sessions. It will also be used to administer score on assessments as well as credentials.

2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d) is as follows:

Please see the attached.

3. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed); is as follows:

Please see the attached.

4. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; is as follows

Please see the attached.

5. The data will be protected using encryption while in motion and at rest as follows:


Please see the attached.

6. The Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and will promptly notify DISTRICT of any such breaches or unauthorized disclosures, as follows:

Please see the attached.

## **Signatures**

For The Vendor:

Signature:  \_\_\_\_\_


Printed Name: Alicia Garcia

Title: Director, Education & Training

Contact Information: agarcia@aws.org

Date: 11/14/2023

For The District:

Signature:  \_\_\_\_\_

Printed Name: Rob McKenzie

Title: Data Protection Officer

Contact Information: dpo@gstboces.org

Date: 11/15/2023

Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.

A. Align Security and Privacy

1. Create a data map to document where data exists and who has access to the data
2. Discover sensitive data to understand where PII or other sensitive information exists
3. Identify Data Owners to help streamline data access governance workflows
4. Monitor how data is moving and being shared throughout the environment
5. Identify and remediate data risks

B. Least Privilege Access = Implement a Least Privilege Access model to ensure that access to sensitive data is minimized

C. Privacy by Design (PbD) principle = adopt a systematic approach to embedding privacy into all design as an essential component of any functionality being delivered

1. Perform regular risk assessments to ensure to minimize any impact or risk to privacy
2. Collect the minimum amount of personal data necessary, ensuring data retention policies and data security measures are in place
3. Provide transparency to end-users through adequate notifications and granular opt-in capabilities

Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.

A. Administrative Safeguards: AWS trains all personnel who engage with PII on the best practices for information handling

B. Physical Safeguards: AWS implements physical protections to safeguard private information including ensuring paper records and servers are secured and access-controlled at all times

C. Technical Safeguards: AWS utilizes technology-based instruments and procedures to protect private information including requiring login credentials for system access and encrypting computers and emails

All AWS employees who engage with PII are trained on best practices to safely handle sensitive information. Specifically:

Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.

- They are required to pass [Cyber Awareness Challenge PII training](#), before allowed access to networks.
- AWS employees, including contractors, will complete an annual PII training, such as [the Safeguarding Personally Identifiable Information \(PII\) Training and the Privacy Act Overview Training](#).
- AWS will maintain records of completion by any method, (e.g., digital using a spreadsheet log or analog using paper documents)
- AWS personnel who mishandle PII are required to take remedial training.

Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum. Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the client.

All AWS employees and subcontractors who engage with PII are bound by written agreement to follow the best practices before they are allowed access to any data.

If AWS experiences a data breach, our protocol is to:

#### A. Secure all operations

1. Act quickly to secure our systems and fix vulnerabilities that may have caused the breach. Secure physical areas potentially related to the breach. Lock them and change access codes, if needed.
2. Mobilize our breach response team immediately to prevent additional data loss.
3. Assemble a team to conduct a comprehensive breach response.
4. Stop additional data loss by taking all affected equipment offline immediately — but don't turn any machines off until the forensic experts arrive. Closely monitor all entry and exit points, especially those involved in the breach. If possible, put clean machines online in place of affected ones. In addition, update credentials and passwords of authorized users.
5. Remove improperly posted information from the web.
  - a. AWS website: If the data breach involved personal information improperly posted on our website, we will remove it immediately.
  - b. Other websites: We will search for the exposed AWS data to make sure that no other websites have saved a copy. If we find any, we will contact those sites and ask them to remove it.
6. Interview people who discovered the breach.
7. We will not destroy evidence collected in the course of our investigation and remediation.

#### B. Fix Vulnerabilities

1. If service providers were involved, AWS will examine what personal information they can access and will decide if their access privileges need to be modified. In addition, AWS will ensure that our service providers take all necessary steps to make sure another breach does not occur. Once our service providers remedy any vulnerabilities, AWS will verify and document.
2. AWS will check our network segmentation. This is done so a breach of one server or in one site does not lead to a breach on another server or site.

#### C. Notify Appropriate Parties

Describe how data will be transitioned to the client when no longer needed by you to meet your contractual obligations, if applicable. Describe your secure destruction practices and how certification will be provided to the client.

1. AWS communications plan. We will use our comprehensive plan that reaches all affected audiences — employees, customers, members, business partners, and other stakeholders. We will not make misleading statements about the breach and will not

2. Notify law enforcement. AWS will contact the local police department immediately. We will report our situation and the potential risk for identity theft.

All PII AWS collects is provided by the EA. As such, AWS will discard all PII according to our data governance policy (See the answer below).

The AWS Data Lifecycle is as follows:



## Data Lifecycle

Capture = AWS is provided with PII by EA.

Organize = AWS will manage all PII that is stored behind login credentials.

Utilize = AWS will use PII for educational purposes only.

Manage = AWS will administer data consistently with all laws and regulations Destroy = AWS will discard all data after 5 years after registration.

AWS will use the following Best Practices for Data Destruction:

1. When drafting written agreements with third parties, AWS includes provisions that specify that all PII that was provided to the third party must be destroyed when no longer needed for the specific purpose for which it was provided, including any copies of the PII that may reside in system backups, temporary files, or other storage media.

2. AWS ensures accountability for destruction of PII by using certification forms which are signed by the individual responsible for performing the destruction and contain detailed information about the destruction.

3. Remember that PII may also be present in non-electronic media. AWS will manage non-electronic records in a similar fashion to their electronic data. When data are no longer required, AWS will destroy non-electronic media using secure means to render it safe for disposal or recycling. Commonly used methods include cross-cut shredders, pulverizers, and incinerators.

4. Depending on the sensitivity of the data being shared, AWS will specify in the written agreement as to the type of destruction to be carried out.

5. When destroying electronic data, AWS will use appropriate data deletion methods to ensure the data cannot be recovered

6. AWS avoids using file deletion, disk formatting, and “one way” encryption to dispose of sensitive data because these methods are not effective as they

leave the majority of the data intact and vulnerable to being retrieved by a determined person with the right tools.

7. AWS will destroy CDs, DVDs, and any magneto-optical disks by pulverizing, cross-cut shredding, or burning.

8. AWS will address in a timely manner sanitization of storage media which might have failed and need to be replaced under warranty or service contract.

9. AWS will create formal, documented processes for data destruction within our organization and require that partner organizations do the same. The data security and privacy program/practice of AWS were developed to complement our current FERPA policy as well as EA's guidance.