# EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed.
   (i) Complaints should be submitted to the EA at: CA BOCES Data Privacy Officer, 1825 Windfall Road, Olean, New York, 14760, via email at DPO@caboces.org or by using the form available at https://caboces.org/resources/new-york-state-education-law-2d/report-an-improper-disclosure/.
   (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

| CONTRACTOR | |
|---|---|
| **Signature:** Pedro Cevallos | <-- Signature to the left |
| **Printed Name:** | Pedro Cevallos |
| **Title:** | Head of Business Development, Educational Services |
| **Date:** | 2/8/2022 |

## EXHIBIT B

### BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) 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** | American Welding Society (AWS) |
| **Description of the purpose(s) for which Contractor will receive/access PII** | Grades for students in welding courses (SENSE schools) and completion rates. |
| **Type of PII that Contractor will receive/access** | Check all that apply:<br>☑ Student PII<br>□ APPR Data<br>□ Does not collect either |
| **Contract Term** | Contract Start Date 2/8/2022<br>Contract End Date 12/31/2025 |
| **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)<br>□ Contractor will not utilize subcontractors.<br>☑ Contractor will utilize subcontractors. |
| **Data Transition and Secure Destruction** | Upon expiration or termination of the Contract, Contractor shall:<br>• Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.<br>• 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 the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request. |

| | |
|---|---|
| **Secure Storage and Data Security** | Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)<br>□ Using a cloud or infrastructure owned and hosted by a third party.<br>☑ Using Contractor owned and hosted solution<br>□ Other:<br>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:<br>Best practices in data governance and privacy protection will be used. |
| **Encryption** | Data will be encrypted while in motion and at rest. |

| **CONTRACTOR** | |
|---|---|
| **Signature:** Pedro Cevallos | <-- Signature to the left |
| **Printed Name:** | Pedro Cevallos |
| **Title:** | Head of Business Development, Educational Services |
| **Date:** | 2/8/2022 |

# EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

## CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

| | | |
|---|---|---|
| 1 | Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract. | A. Align Security and Privacy<br>1. Create a data map to document where data exists and who has access to the data<br>2. Discover sensitive data to understand where PII or other sensitive information exists<br>3. Identify Data Owners to help streamline data access governance workflows<br>4. Monitor how data is moving and being shared throughout the environment<br>5. Identify and mitigate data risks<br>B. Least Privilege Access = Implement a Least Privilege Access model to ensure that access to sensitive data is minimized<br>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<br>1. Perform regular risk assessments to ensure to minimize any impact or risk to privacy<br>2. Collect the minimum amount of personal data necessary, ensuring data retention policies and data security measures are in place<br>3. Provide transparency to end-users through adequate notification and granular opt-in activities. |
| 2 | 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<br>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<br>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<br>All AWS employees who engage with PII are trained on best practices to safely handle sensitive information. |
| 3 | 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. | 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. Specifically:<br>• They are required to pass Cyber Awareness Challenge PII training, before allowed access to networks.<br>• AWS employees, including contractors, will complete an annual PII training, such as the Safeguarding (https://public.cyber.mil/training/cyber-awareness-challenge/) Personally Identifiable Information (PII) Training and the Privacy Act Overview Training (https://public.cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii-v4/).<br>• AWS will maintain records of completion by any method, (e.g., digital using a spreadsheet log or analog using paper documents)<br>• AWS personnel who mishandle PII are required to take remedial training. |
| 4 | 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. | 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. Specifically:<br>• They are required to pass Cyber Awareness Challenge PII training, before allowed access to networks.<br>• AWS employees, including contractors, will complete an annual PII training, such as the Safeguarding (https://public.cyber.mil/training/cyber-awareness-challenge/) Personally Identifiable Information (PII) Training and the Privacy Act Overview Training (https://public.cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii-v4/).<br>• AWS will maintain records of completion by any method, (e.g., digital using a spreadsheet log or analog using paper documents)<br>• AWS personnel who mishandle PII are required to take remedial training. |
| 5 | 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 EA. | If AWS experiences a data breach, our protocol is to:<br>A. Secure all operations<br>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.<br>2. Mobilize our breach response team immediately to prevent additional data loss.<br>3. Assemble a team to conduct a comprehensive breach response.<br>B. Fix Vulnerabilities<br>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.<br>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.<br>C. Notify Appropriate Parties |

| | | |
|---|---|---|
| 6 | Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable. | The AWS Data Lifecycle is as follows:<br>Capture = AWS is provided with PII by EA.<br>Organize = AWS will manage all PII that is stored behind login credentials.<br>Utilize = AWS will use PII for educational purposes only.<br>Manage = AWS will administer data consistently with all laws and regulations<br>Destroy = AWS will discard all data after 7 years after their last use.<br>AWS will use the following Best Practices for Data Destruction. |
| 7 | Describe your secure destruction practices and how certification will be provided to the EA. | AWS will use the following Best Practices for Data Destruction:<br>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.<br>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.<br>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.<br>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.<br>5. When destroying electronic data, AWS will use appropriate data deletion methods to ensure the data cannot be recovered<br>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. |
| 8 | Outline how your data security and privacy program/practices align with the EA's applicable policies. | The security and privacy policies at AWS are based on the EA's policies as well as best practices for data governance. |
| 9 | Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below. | PLEASE USE TEMPLATE BELOW. |

## EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies ); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional

| Function | Category | Contractor Response |
|---|---|---|
| IDENTIFY (ID) | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | |
| | **Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. | |
| | **Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | |
| | **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | |
| | **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | |
| | **Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks. | |

| Function | Category | Contractor Response |
|---|---|---|
| PROTECT (PR) | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | |
| | **Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. | |
| | **Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. | |
| | **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. | |
| | **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. | |
| | **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. | |
| DETECT (DE) | **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | |
| | **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | |

| Function | Category | Contractor Response |
|---|---|---|
|  | **Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. |  |
| RESPOND (RS) | **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. |  |
|  | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). |  |
|  | **Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities. |  |
|  | **Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. |  |
|  | **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. |  |

| Function | Category | Contractor Response |
|---|---|---|
| RECOVER (RC) | **Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. | |
| | **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | |
| | **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g.  coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). | |