## 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** | CastleBranch, Inc.<br>_____ |
| **PII Declaration** | **Does your organization/software collect student personally identifiable information (PII) or staff PII?**<br><br>Examples of student PII:<br><br>a. The student's name;<br>b. The name of the student's parent or other family members;<br>c. The address of the student or student's family;<br>d. A personal identifier, such as the student's social security number, student number, or biometric record;<br>e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name;<br><br>Examples of staff APPR PII:<br><br>a. Teacher ID<br>b. Name<br>c. Birthdate<br>d. Gender<br>e. Race<br>f. Salary<br><br>☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.<br><br>If you collect the PII information above, please complete the remainder of this form. |
| **Description of the purpose(s) for which Contractor will receive/access PII** | CastleBranch can receive PII thorugh multiple ways depending on how the client would like to deliever the data. The most used is through web application, which uses TLS 1.2 encryption protocol, and the client, either student or staff enters their infromation into the web app. The second is through bulk data movement through secure API. |
| **Type of PII that Contractor will receive/access** | Check all that apply:<br>☑ Student PII<br>☑ APPR PII |

| | |
|---|---|
| **Contract Term** | Contract Start Date 10/01/2022<br>Contract End Date 06/30/2023 |
| **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><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>CastleBranch takes great lengths to keep data secure. The company uses AWS IaaS and connects to them through secure connections including VPN |
| **Encryption** | Data will be encrypted while in motion and at rest. |

## 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. | CastleBranch is required to adhere to PCI DSS and is SOC 2 type 2 audited with those compliance pieces. Not withstanding regulatory pieces of FERPA, GDPR, and FCRA. We value security very highly and follow several different framework that are NIST and CIS |
| 2 | Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII. | CastleBranch operates on the Principle of Least Privilege, data is secured in tranist using TLS 1.2 and at rest using AES 256. |
| 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. | CastleBranch employees are required to be up-to-date quarterly on their monthly security awareness training. Further, new hires are onboarded with security awareness. Finally, dependent on the role and what data is handled by the employee, stringent PII handling 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. | CasIteBranch requires employees to sign security awareness training forms, acceptable use form, NDA, and confiedntiality agreements. |
| 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. | CastleBranch has adapted NIST Special Publication 800-61r2 for breach protocols. Depending on severity of the privacy and/or security incident bases how CastleBranch responds to the event.<br>Small, accidental privacy incidents are logged, documented and corrected ASAP, depending on size and scope, individuals and clients are notified.<br>Large incidents and any security breaches are documented, tracked, adn resolved.<br>Notifications follow all necessary laws and regulations. |
| 6 | Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable. | Data can be tranisitioned depending on how it would like to be received. Preferred is XML |
| 7 | Describe your secure destruction practices and how certification will be provided to the EA. | CastleBranch utilizes NIST 800-88 for their data destruction policy. The company uses a third party to handle physical media destruction. CastleBranch does not share certificate of destruction |
| 8 | Outline how your data security and privacy program/practices align with the EA's applicable policies. | CastleBranch does not know, and has not seen EA's policies. CastleBranch's policies follow NIST, CIS, and SANs frameworks. |
| 9 | Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 | CastleBranch strives to consistently better with regards to cyber security. With the statement above regarding that policies follow NIST, CIS, and SANs frameworks, CastleBranch can say that it follows NIST CSF 1.1. Following the SOC audit controls, PCI DSS, and CIS Risk Assessment Controls, Asset Based can further |

# Western Suffolk BOCES 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: dpo@wsboces.org. (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]** | Tom Cucuel |
| **[Printed Name]** | Tom Cucuel |
| **[Title]** | COO |
| **Date:** | 08/23/2022 |