

**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	Stefanie Kessen
Description of the purpose(s) for which Contractor will receive/access PII	To set up online accounts and receive payment
Type of PII that Contractor will receive/access	Check all that apply: <input type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date <u>07/01/2021</u> Contract End Date <u>06/30/2022</u>
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) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • 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. • 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)

- Using a cloud or infrastructure owned and hosted by a third party.
- Using Contractor owned and hosted solution
- Other: Kajabi

Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:

Platform is run through Kajabi, who mitigates security and privacy in a manner that does not compromise security of data. For more information, go to www.Kajabi.com

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.	Kajabi takes reasonable measures to protect personal information and content and to ensure that your content remains protected and available to you.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Only authorized employees have access to the administrative side of the website and only the owner has access to personal information from members (payment info)
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.	Authorized employees receive training on the confidentiality of PII and the federal and state laws that govern the confidentiality of PII
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.	Employees and subcontractors sign a written agreement to the requirements of their contract, including the understanding and agreement to follow the federal and state laws that govern the confidentiality of PII.
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.	Kajabi mitigates any data/privacy incidents and implicate PII. If there are any breaches or unauthorized disclosures, there will be immediate communication with any customer within our system.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data is purged and deleted after 2 years of no activity from a customer.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Kajabi's platform and policy will used for the destruction of old records
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	We transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Kajabi independently follows the security and privacy practices outlined in NIST CSF v1.1

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	
	Verified by PDFfiller
[Signature]	
[Printed Name]	10/14/2021 Stefanie Kessen
[Title]	Owner/President
Date:	10/14/2021

March 30, 2021



PDFfiller Document ID: 9C48-3191-CE12-0003