

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	Gimkit, Inc. <hr/>
PII Declaration	<p>Does your organization/software collect student personally identifiable information (PII) or staff PII?</p> <p>Examples of student PII:</p> <ul style="list-style-type: none"> a. The student’s name; b. The name of the student’s parent or other family members; c. The address of the student or student’s family; d. A personal identifier, such as the student’s social security number, student number, or biometric record; e. Other indirect identifiers, such as the student’s date of birth, place of birth, and Mother’s Maiden Name; <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"> a. Teacher ID b. Name c. Birthdate d. Gender e. Race f. Salary <p><input type="checkbox"/> IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</p> <p>If you collect the PII information above, please complete the remainder of this form.</p>
Description of the purpose(s) for which Contractor will receive/access PII	Gimkit is an online formative assessment tool. The information we collect is used exclusively for the purpose of building, improving, and maintaining Gimkit.
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR PII

Contract Term	Contract Start Date <u>06/06/2023</u> Contract End Date <u>06/06/2026</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) <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other:
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

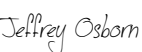
The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a 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.	Gimkit will implement applicable state, federal, and local data security and privacy contract requirements over the life of the Contract and only use PII in accordance with the Contract, and applicable laws pertaining to data privacy and security including Education Law § 2-d.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Gimkit shall comply with all District and Board of Education policies as well as state, federal, and local laws, regulations, rules, and requirements related to the confidentiality of records and data security and privacy, including the District's Parents' Bill
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.	Gimkit will provide annual training to its officers, employees, or assignees who have access to PII on the federal and state law governing confidentiality of such data.
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.	Contractor will ensure that its employees, with whom Contractor shares PII, abide by all applicable data protection and security requirements by entering into written agreements whereby such parties will perform their obligations in a manner consistent with the data protection and security requirements outlined therein.
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.	Upon the discovery of a breach of security that results in the unauthorized release, disclosure or acquisition of personal information, we will notify electronically, not later than 48 hours, such discovery to all affected Users so that you can take appropriate protective steps. This initial notice will include, to the extent known at the time of the notification, the date and time of the breach, its nature and extent, and our plan to investigate and remediate the breach. Contractor will cooperate with EA and law enforcement to protect the integrity of investigations into the Breach as provided in the
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon expiration or termination of the Contract, Contractor shall transfer PII to EA, in a mutually agreed upon format, provided that EA has made such a written request at the expiration or termination of the Contract.
7	Describe your secure destruction practices and how certification will be provided to the EA.	PII will be securely destroyed within 30 days of expiration or termination of the Contract utilizing an approved method of confidential destruction, including verified erasure of magnetic media using approved methods of electronic file destruction. Hereafter, Contractor will provide EA with certification of such destruction.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor will implement the data protection and security requirements as a Third-Party Contractor as outlined in 8 NYCRR Part 121 and in accordance with the EA's Policy, as well as include EA's Parents Bill of Rights and Supplemental Information to the Service Agreement.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	See attached completed template

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]	
[Printed Name]	Jeffrey Osborn
[Title]	Co-Founder
Date:	06/06/2023

January 13, 2022



PDFfiller Document ID: BEE5-4CC9-E103-0000

CONTRACTOR’S DATA SECURITY AND PRIVACY 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.	Contractor will implement applicable state, federal, and local data security and privacy contract requirements over the life of the Contract and only use PII in accordance with the Contract, and applicable laws pertaining to data privacy and security including Education Law § 2-d.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Gimkit shall comply with all District and Board of Education policies as well as state, federal, and local laws, regulations, rules, and requirements related to the confidentiality of records and data security and privacy, including the District’s Parents’ Bill of Rights for Data Privacy and Security, annexed hereto. Additionally, We use industry best practices to securely store and transmit user information. Specifically, all Gimkit data is encrypted at motion and at rest under the highest current industry standards (TLS/SSL). We force HTTPS on our site, which means that it is not possible for a third party to see data between the client side and Gimkit. Gimkit's data at rest is stored in a database, in which the only way to access it is by having

		Gimkit's database credentials. We force all web traffic on gimkit.com to use HTTPS.
3	Address the training received by your employees, officers and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Contractor will provide annual training to its officers, employees, or assignees who have access to PII on the federal and state law governing confidentiality of such data.
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.	Contractor will ensure that its employees, with whom Contractor shares PII abide by all applicable data protection and security requirements by entering into written agreements whereby such parties will perform their obligations in a manner consistent with the data protection and security requirements outlined therein.
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.	<p>Upon the discovery of a breach of security that results in the unauthorized release, disclosure or acquisition of personal information, we will notify electronically, not later than 48 hours, such discovery to all affected Users so that you can take appropriate protective steps. This initial notice will include, to the extent known at the time of the notification, the date and time of the breach, its nature and extent, and our plan to investigate and remediate the breach.</p> <p>Contractor will cooperate with EA and law enforcement to protect the integrity of investigations into the Breach as provided in the DPA.</p>

6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon expiration or termination of the Contract, Contractor shall transfer PII to EA, in a mutually agreed upon format, provided that EA has made such a written request at the expiration or termination of the Contract.
7	Describe your secure destruction practices and how certification will be provided to the EA.	PII will be securely destroyed within 30 days of expiration or termination of the Contract utilizing an approved method of confidential destruction, including verified erasure of magnetic media using approved methods of electronic file destruction. Thereafter, Contractor will provide EA with certification of such destruction.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor will implement the data protection and security requirements as a "Third-Party Contractor" as outlined in 8 NYCRR Part 121 and in accordance with the EA's Policy, as well as include EA's Parents Bill of Rights and Supplemental Information to the Service Agreement.
9	<p>Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.</p> <p>OR</p> <p>Outline how your data security and privacy program/practices materially align with the NIST CSF v 1.1. Please include details regarding how you will identify, protect, respond to, and recover from data security and privacy threats, as well as how you will manage your security controls</p>	PLEASE USE TEMPLATE BELOW.

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 pages if needed.

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.	2
	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.	2
	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.	2
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions,	2

	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.	2
	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.	2
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.	7
	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.	5
	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.	5
	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.	5
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are	7

	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.	2
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	7
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	2
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	2
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	2
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	5
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	2
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	2
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	5
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.	2

	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	2
	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).	2