

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and **Gimkit, Inc.** (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Shoreham-Wading River Central School District (the "District") and Contractor to the contrary, Contractor agrees as follows:

1. Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third-parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by New York State ("State") or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

2. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Contractor's Data Security and Privacy Plan Requirements

3. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:
 - a. Outline how the Contractor will implement all State, federal, and local data security and privacy requirements over the life of the Agreement, consistent with the District's data security and privacy policy;
 - b. Specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
 - c. Demonstrate Contractor's compliance with the requirements of 8 NYCRR Part 121.3(c);
 - d. Specify how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and State laws governing confidentiality of such data prior to receiving access;
 - e. Specify how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
 - f. Specify how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
 - g. Describe whether, how and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the Agreement is terminated or expires.
4. Pursuant to the Plan, Contractor will:
 - a. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5;

- b. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
- c. Limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
- d. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
- e. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
 - i. except for authorized representatives of Contractor such as a subcontractor or assignee to the extent they are carrying out the Agreement and in compliance with State and federal law, regulations and its Agreement with District; or
 - ii. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.
- f. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
- g. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
- h. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Contractor understands and agrees that it is responsible for submitting the above-referenced Data Security and Privacy Plan to the District prior to the start of the term of this Agreement. A copy of Contractor's Data Security and Privacy Plan is attached hereto as Exhibit "C". Further, Contractor shall sign a copy of the District's Parents Bill of Rights attached hereto as Exhibit "A".

Contractor's Supplemental Information Requirements

5. Contractor understands that, as part of the District's obligations under New York State Education Law § 2-d, Contractor is responsible for providing the District with supplemental information to be included in the District's Parents' Bill of Rights. Such supplemental information shall include:

- a. The exclusive purposes for which the student data or teacher or principal data will be used;
- b. How the Contractor will ensure that the subcontractors, persons or entities that the Contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
- c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the Agreement;
- d. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
- e. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The supplemental information required to be provided is included as Exhibit “B” and is incorporated by reference herein and made a part of this Agreement.

6. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data or teacher or principal data, Contractor shall immediately notify the District and advise it as to the nature of the breach and steps Contractor has taken to minimize said breach. Said notification must be made in the most expedient way possible and without unreasonable delay but within no more than seven (7) calendar days of discovery of the breach. Notification required hereunder shall be made in writing and must, to the extent available, include a description of the breach, date of incident, date of discovery, the types of personally identifiable information affected, the number of records affected, a description of Contractor’s investigation, and contact information for Contractor’s representatives who can assist the District. Notification must be sent to the District’s Superintendent of Schools with a copy to the District’s Data Protection Officer. Notifications required under this paragraph must be provided to the District. at the following address:

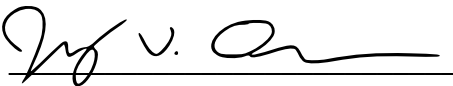
Mr. Gerard Poole
Shoreham-Wading River Central School District
250B Rt. 25A
Shoreham, NY 11786

7. In the event that Contractor fails to notify the District of a breach in accordance with Education Law § 2-d, and/or Part 121 of the Regulations of the Commissioner of Education, said failure shall be punishable by a civil penalty of the greater of five thousand dollars (\$5,000) or up to ten dollars (\$10) per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).
8. Except as provided in Education Law § 2-d(6)(d), in the event Contractor violates Education Law § 2-d, said violation shall be punishable by a civil penalty of up to one

thousand dollars (\$1,000). A second violation involving the same data shall be punishable by a civil penalty of up to five thousand dollars (\$5,000). Any subsequent violation involving the same data shall be punishable by a civil penalty of up to ten thousand dollars (\$10,000). Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

9. Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a breach. Any costs incidental to the required cooperation or participation of the Contractor or its employees, agents, affiliates, or authorized users, as related to such investigations, will be the sole responsibility of the Contractor if such breach is attributable to the Contractor or its subcontractors.
10. Upon termination of this Agreement, Contractor shall return or, at the District's option, destroy all confidential information obtained in connection with the services provided herein and/or Protected Data. Destruction of the confidential information and/or Protected Data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. Contractor further agrees that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.
11. In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Contractor by State and federal law and Agreement shall apply to the subcontractor.
12. Where a parent or eligible student requests a service or product from Contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party Contractor for purposes of providing the requested product or service, such use by the third-party Contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor: Gimkit, Inc.

Signature: 

Date: 5/13/2025

EXHIBIT “A”

Shoreham-Wading River Central School District Parents’ Bill of Rights

Parents and guardians of students attending or seeking to enroll in the Shoreham-Wading River CSD are advised that they have the following rights with regard to student data under New York State Education Law.

1. A student’s personally identifiable information will not be released or sold by the District for any commercial purposes.
2. A parent or guardian has the right to inspect and review the complete contents of their child’s education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred. Third Party contractors are required to employ technology, safeguards, and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.
4. A complete list of all student data elements collected by New York State is available for public review at <https://www.nysed.gov/data-privacy-security/student-data-inventory> or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
5. Parents and guardians have the right to have complaints about possible breaches of student data addressed. 89 Washington Avenue Albany, NY 12234

Complaints should be addressed to:

Alan Meinster, Assistant Superintendent for Curriculum, Instruction, and Assessment; DPO

250B Route 25A
Shoreham, NY 11786
(631) 821-8100

Or with NYSED

Chief Privacy Officer

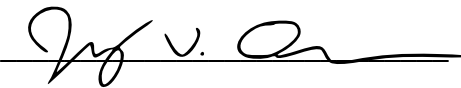
New York State Education Department

Email: Privacy@nysed.gov

6. This Bill of Rights will be included with every contract entered by the District with an outside contractor if the contractor will receive student, teacher, or principal data. This Bill of Rights will be supplemented to include information about each contract that the District enters into with an outside contractor receiving confidential student, teacher, or principal data, including the exclusive purpose (s) for which the data will be used, how the contractor will ensure confidentiality and data protection and security requirements, the date of expiration of the contract and what happens to the data upon the expiration of the contract, if and how the accuracy of the data collected can be challenged, where the data will be stored and the security protections that will be taken.
7. In the event of a data breach or unauthorized disclosure of students’ personally identifiable information, third party contractors are required by law to notify the School District within seven (7) days of discovery of the breach or unauthorized disclosure.

8. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, the District will notify the public via written notice, electronic notice through the District's electronic communication platform, or Telephone notification.
9. 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.
10. Parents may access the State Education Department's Parent's Bill of Rights at: https://www.nysed.gov/sites/default/files/programs/data-privacy-security/parents-bill-of-rights_2.pdf

Contractor: Gimkit, Inc.

Signature: 

Date: 5/13/2025

EXHIBIT "B"
Contractor's Supplemental Information

| | |
|---|--|
| Name of Contractor | Gimkit, Inc. |
| Description of the purpose(s) for which Contractor will receive/access PII | The information we collect is used exclusively for the purpose of building and maintaining Gimkit. |
| Type of PII that Contractor will receive/access | Check all that apply: <input checked="" type="checkbox"/> Student PII <input checked="" type="checkbox"/> APPR Data |
| Agreement Term | Agreement Start Date: <u>5/1/2025</u> Agreement End Date: <u>4/30/2028</u> |
| Subcontractor Written Agreement Requirement | Contractor will not utilize subcontractors without a written agreement 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 Agreement. (check applicable option): <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" 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 District, or a successor contractor at the District'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 District. If a correction to data is deemed necessary, the District will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the District's written request. |

| | |
|---|---|
| Secure Storage and Data Security | <p>Please describe where PII will be stored and the protections taken to ensure PII will be protected (check all that apply):</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third-party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution.</p> <p><input type="checkbox"/> Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> |
| Encryption | <p>Data will be encrypted while in motion and at rest.</p> |

Contractor: Gimkit, Inc.

Signature: _____

Date: 5/13/2025

EXHIBIT “C”
Contractor’s Data Security & Privacy Plan

CONTRACTOR’S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

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 and FERPA. |
| 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. Training is provided on an ongoing basis online to employees (there are 2). Records kept in Basecamp. |
| 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. | Gimkit ensures that its employees, and subcontractors in the form of trusted third parties, with whom it 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 24 hours, such discovery to all affected districts 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. |