DATA PRIVACY AND SECURITY PLAN

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

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

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.

and at rest

Additionally, We use industry best practices to securely store and transmit user information. Specifically, all Gimkit data is encrypted in motion. 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. Gimkit data is encrypted at motion and at rest under the highest current industry standards (TLS/SSL)

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

Gimkit does not allow action on Gimkit accounts without proof of account ownership, including providing the account's unique support token or driver's license if the account owner cannot access the account.

3. Specifies 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;

Gimkit has three (3) employees. All are trained regularly on best practices for data collection and handling as laws and guidelines are changed and adjusted. We stay up to date on the most recent updates and best practices..

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

Gimkit does not utilize subcontractors.

5. Specifies 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 educational agency;

Although we make a concerted good faith effort to maintain the security of personal information, and we work hard to ensure the integrity and security of our systems as per best industry standards, no practices are 100% immune, and we can't guarantee the security of information. Outages, attacks, human error, system failure, unauthorized use or other factors may compromise the security of User information at any time. If such event were to happen this is how we would respond:

Initial Notice: 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.

Detailed Notification: Upon discovery of a breach, we will conduct a deep investigation in order to electronically provide, not later than 5 days, all affected Users with a more detailed notice of the breach, including but not limited to the date and time of the breach; nature and extent of the breach; and measures taken to ensure that such breach does not occur in the future. We may also post a notice on our homepage (www.gimkit.com) and, depending on where you live, you may have a legal right to receive notice of a security breach in writing. Where, and in so far as, it is not possible to provide all of the aforementioned information at the same time, we will provide you with the remaining information without undue further delay.

Both notifications will be written in plain language, will be titled "Notice of Data Breach" and will present the information described above under the following heading: "What Happened", "What Information Was Involved", "What We Are Doing", "What You Can Do" and "For More Information." Additional information may be provided as a supplement to the notice.

6. Specifies whether Protected 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 contract is terminated or expires.

How We Handle Personal Information:
We take all measures reasonably necessary to protect against the unauthorized access, use, alteration, or destruction of potentially personally-identifying information. We disclose potentially personally-identifying information only on an as-needed (or required) basis as follows:

With our employees that: (i) need to know that information to process it on our behalf or to provide the Services; and (ii) that have expressly agreed not to disclose it to others.
As required by law (including but not limited to COPPA and FERPA regulations) such to comply with a subpoena or similar legal process. To the extent we are legally permitted to do so, we will take commercially reasonable steps to notify you if we are required to provide your personal information to third parties as part of a legal process.

When we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a written government request
If we become involved in a merger, acquisition, or any form of sale of some or all of its assets. In the event of a merger, acquisition, or any form of sale of some or all of our assets, we will ensure that the acquiring organization agrees to protect personal information in accordance with the commitments we have made in this Privacy Policy, and that the acquiring organization will provide notice before personal information, customer information, or business information becomes subject to a different privacy notice.

To add on to the above, if a school or district did provide any data to Gimkit directly, that data would be returned to them in the form they require/request at the end of a contract and 3 months after early termination.