Parents Bill of Rights Relating to Student Data

The District, in compliance with Education Law 2-d, provides the following:

DEFINITIONS:
As used in this policy, the following terms are defined:

Student Data means personal identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records 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.

Third-Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or Principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization other than a District.

1. Neither student data, nor teacher or Principal data will not be sold or released for any commercial purpose;

2. Parents have the right to inspect and review the complete contents of their child's education record. Procedures for reviewing student records can be found in the Board Policy entitled: **#26 Policies and Procedures and Family Educational Rights and Privacy Act (FERPA) Notice for Directory Information** – *Section 1 – Legally Mandated Policies*;

3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to encryption, firewalls, and password protection. As required by Education Law §2-d(5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) is adopted as the standard for data security and privacy;

4. New York State maintains a complete list of all student data collected by the State and the data is available for public review at http://www.p12.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx 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 have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to Records Access Officer, Joseph

Gugino, Oxford Academy and Central School District, PO Box 192, Oxford, NY 13830;

6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;

- Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;

- Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District hall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;

- The District will require complaints to be submitted in writing;

- The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1;

7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or Principal data. The supplemental information must be developed by the District and include the following information:

- The exclusive purposes for which the student data or teacher or Principal data will be used by the third-party contractor, as defined in the contract;

- How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or Principal data, if any, will abide by all applicable data protection and security requirements, including, but not limited to, those outlined in applicable State and federal laws and regulations (e.g., FERPA; Education Law §2-d);

- The duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or Principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District and whether, when and how the data will be destroyed);

- If an 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;

- Where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed

using encryption while in motion and at rest will be addressed.

8. This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third party contractor where the third party contractor receives student data or teacher or Principal data.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name Gimkit, INC. Product Name Gimkit

Printed Name Jeffrey Osborn Signature _____ Date 8/11/20

Adopted 5/9/16

Amended 6/1/20

Hogan, Sarzynski, Lynch, DeWind & Gregory, LLP 7/2014

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.

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.

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.

Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D

Oxford Academy and Central School and the Third-Party Contractor agree as follows:

1. Definitions:
    a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
    b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and the Oxford Academy and Central School's Data Security and Privacy Policy;

3. The Parties agree that the Oxford Academy and Central School's Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;

4. The Third-Party Contractor agrees to comply with New York State Education Law §2-d and its implementing regulations;

5. The Third-Party Contractor agrees that any officers or employees of the Third-Party Contractor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;

6. The Third-Party Contractor shall:
    a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
    b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
    c. except for authorized representatives of the Third-Party Contractor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
        i. without the prior written consent of the parent or eligible student; or
        ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
    d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
    e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human

Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;

f. adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework;

g. impose all the terms of this rider in writing where the Third-Party Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name Gimkit, INC. Product Name Gimkit

Printed Name Jeffrey Osborn Signature  Date 8/11/20