SOFTWARE VENDOR AGREEMENT

This Agreement, made and entered into on 4/16/2024 (Effective Date), by and between Gimkit, Inc. ("[ ]"), with a main office at 2716 3rd Ave N, Seattle, WA 98109 ("Vendor"), and the Baldwinsville Central School District, having an office at 29 East Oneida Street, Baldwinsville, New York 13027 ("School District") (collectively "Parties").

In consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1. Services. Vendor shall perform the services set forth in this Agreement, as described in Addendum A (the "Services"). Vendor shall provide the Services at the School District location or on a remote basis, as agreed to by the Parties. Vendor warrants that the Services provided hereunder will be performed in a good and workmanlike manner.

2. Data Accessed by Vendor. Vendor shall identify categories of all data accessed by Vendor or its subcontractors as part of this Agreement as set forth in Addendum B.

3. **Term of Services**. This Agreement begins on the Effective Date and will continue for a period of 3 years unless terminated pursuant to Section 4 below (the "Term").

4. Termination. This Agreement may be terminated as follows:

(a) By the School District upon thirty (30) days prior written notice to Vendor;

(b) By the School District immediately in the event of breach by the Vendor; and

(c) By either Party upon written mutual agreement.

5. Payment. Payment shall be made in accordance with Addendum C attached hereto.

6. Protection of Confidential Data. Vendor shall provide its Services in a manner which protects Student Data (as defined by 8 NYCRR § 121.1(q)) and Teacher or Principal Data (as defined by 8 NYCRR § 121.1(r)) (hereinafter "Confidential Data") in accordance with the requirements articulated under Federal, State and local laws and regulations, including but not limited to the foregoing:

(a) Vendor will adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(b) Vendor will comply with the School District Data Security and Privacy Policy, Education Law § 2-d, and 8 NYCRR § 121.

(c) Vendor will limit internal access to personally identifiable information to only those employees or subcontractors that need access to provide the contracted services.

(d) Vendor will not use the personally identifiable information for any purpose not explicitly authorized in this Agreement.

(e) Vendor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student, unless otherwise authorized pursuant to applicable law.

(f) Vendor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody.

(g) Vendor will use encryption to protect personally identifiable information in its custody while in motion or at rest.

(h) Vendor will 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.

(i) In the event Vendor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Vendor shall apply to the subcontractor.

7. **Data Breach**. In the event that Confidential Data is accessed or obtained by an unauthorized individual, Vendor shall provide notification to the School District without unreasonable delay and not more than seven (7) calendar days after the discovery of such breach. Vendor shall follow the following process:

(a) The security breach notification shall be titled "Notice of Data Breach," shall be clear, concise, use language that is plain and easy to understand, and to the extent available, shall include: a brief description of the breach or unauthorized release; the dates of the incident and the date of discovery; a description of the types of Confidential Data affected; an estimate of the number of records affected; a brief description of the Vendors investigation or plan to investigate; and contact information for representatives who can assist the School District with additional questions.

(b) The Vendor shall also prepare a statement for parents and eligible students which provides information under the following categories: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."

(c) Where a breach or unauthorized release of Confidential Data is attributed to Vendor, and/or a subcontractor or affiliate of Vendor, Vendor shall pay for or promptly reimburse the School District for the full cost of notification to parents and eligible students of the breach.

(d) Vendor shall cooperate with the School District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Confidential Data.

(e) Vendor further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and Federal and State laws for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Confidential Data or any portion thereof. Upon request, Vendor shall provide a copy of said written incident response plan to the School District.

8. Indemnification. Vendor shall at all times (both during and after the Term of this Agreement), indemnify, defend and hold harmless the School District, its agents, employees, and students (collectively for purposes of this Section, "the School District"), from and against any and all settlements, losses, damages, costs, counsel fees and all other expenses relating to or arising from (a) Vendor's failure to comply with the terms of this Agreement; and/or (b) the negligent operations, acts or omissions of the Vendor.

9. Compliance with Laws. Vendor, its employees and representatives shall at all times comply with all applicable Federal, State and local laws, rules and regulations.

10. Independent Relationship. It is expressly intended by the Parties hereto, and Vendor hereby specifically warrants, represents and agrees, that Vendor and the School District are independent entities. The Parties intend that this Agreement is strictly between two independent entities and does not create an employer/employee relationship for any purpose. Vendor shall perform the duties contemplated by this Agreement as an independent entity, to whom no benefits shall accrue except for those benefits expressly set forth in this Agreement.

11. Assignment. This Agreement is binding upon the Parties and their respective successors and assigns, but Vendor's obligations under this Agreement are not assignable without the prior written consent of the School District. Any assignment without the School District's consent shall be null and void.

12. Governing Law and Venue. This Agreement and any Services provided hereunder shall be governed by the laws of the State of New York both as to interpretation and performance, without regard to its choice of law requirements. Any such action arising hereunder shall be venued in the Supreme Court of the State of New York, County of Onondaga.

13. Waiver. No delay or omission of the School District to exercise any right hereunder shall be construed as a waiver of any such right and the School District reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

14. **Addendums.** The following Addenda are attached hereto and incorporated herein:

- Addendum A: Description of Specifications and Services
- Addendum B: Schedule of Data
- Addendum C: Payment Schedule
- Addendum D: School District's Parents' Bill of Rights
- Addendum E: Parents' Bill of Rights – Supplemental Information Addendum
- Addendum F: Vendor's Data Security and Privacy Plan

15. **Severability**. Should any part of this Agreement for any reason be declared by any court of competent jurisdiction to be invalid, such decision shall not affect the validity of any remaining portion, which remaining portion shall continue in full force and effect as if this Agreement had been executed with the invalid portion hereof eliminated, it being the intention of the Parties that they would have executed the remaining portion of this Agreement without including any such part, parts or portions which may for any reason be hereafter declared invalid.

16. **Entire Agreement**. This Agreement and its Addendums constitute the entire Agreement between the Parties with respect to the subject matter hereof and shall supersede all previous negotiations, commitments and writings. It shall not be released, discharged, changed or modified except by an instrument in writing signed by a duly authorized representative of each of the Parties.

IN WITNESS WHEREOF, the Parties have signed this Agreement intending to be legally bound.

Gimkit, Inc.

By: ______________________

Name: Jeffrey Osborn

Title: Co-Founder

Date: 4/16/2024

Baldwinsville Central School District

By: ______________________

Name: ______________________

Title: ______________________

Date: ______________________

Addendum A

DESCRIPTION OF SPECIFICATIONS AND SERVICES

Description of Services

Gimkit is an online formative assessment tool that makes review fun and engaging for students using gamification.

Product Specifications

> Online only, no Downloads
> Mac OS 10 and Higher
> Windows OS 10 and Higher
> Chrome, Safari, Firefox
> All network adjustments here:
https://help.gimkit.com/en/category/troubleshooting-ecq2l8/

Technical Specifications

See above

Addendum B

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses, Use of cookies etc.	x
	Other application technology meta data (specify):	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data (specify): *Student Personality Assessments*	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information (specify):	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information (specify):	
Parent/ Guardian Contact Information	Address	
	Email	
	Phone	
Parent/ Guardian ID	Parent ID number (created to link parents to students)	

Category of Data	Elements	Check if used by your system
Parent/ Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information(specify): *First Generation College Student*	
Student Contact Information	Address	
	Email	x
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	x
Student In-App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	x
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content, writing, pictures etc.	
	Other student work data (Please specify):	
Transcript	Student course grades	

Category of Data	Elements	Check if used by your system
	Student course data	
	Student course grades/performance scores	
	Other transcript data (Please specify):	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data (Please specify):	
Other	Please list each additional data element used, stored or collected by your application	

Addendum C

PAYMENT SCHEDULE

Addendum D

SCHOOL DISTRICT’S PARENTS’ BILL OF RIGHTS

School districts and BOCES are required to publish an "Education Law §2-d Bill of Rights for Data Privacy and Security".

Parents and eligible students1 can expect the following:

1. A student’s personally identifiable information (PII)2 cannot be sold or released for any commercial purpose.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.

3. State and federal laws, 3 such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act (FERPA), that protect the confidentiality of a student's PII, 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.

4. A complete list of all student data elements collected by the New York State Education Department (NYSED) is available for public review at www.nysed.gov/data-privacy-security, and by writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be submitted to NYSED online at www.nysed.gov/data-privacy-security, 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. Complaints may also be directed to:

RJ DeLisle, Data Protection Officer
Baldwinsville Central School District
29 East Oneida St
Baldwinsville, NY. 13027
Phone: 315-638-6190
Email: rdelisle@bville.org

6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

[1] "Parent" means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. "Eligible Student" means a student 18 years and older.

[2] "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter.

[3] Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data.

Addendum E

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by **Gimkit, Inc.** (the "Vendor") are limited to the purposes authorized in the contract between the Vendor and Baldwinsville Central School District (the "School District") dated **4/16/2024** (the "Contract").

2. **SUBCONTRACTOR OVERSIGHT DETAILS**: The Vendor will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to 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., Family Educational Rights and Privacy Act ("FERPA"); Education Law § 2-d; 8 NYCRR § 121).

3. **CONTRACT PRACTICES**: The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the School District in a mutually agreeable format and/or destroyed by the Vendor as directed by the School District.

4. **DATA ACCURACY/CORRECTION PRACTICES**: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in the FERPA, stored by the School District in Vendor's product and/or used by Vendor's service by following the School District's procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by School District in Vendor's product and/or used by Vendor's by following the appeal procedure in the School District's APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES**: Confidential Data provided to Vendor by the School District will be stored Cloud; USA only. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework, including but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES**: The Vendor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section

2-d and other applicable law.

Addendum F

VENDOR'S DATA SECURITY AND PRIVACY PLAN

[See Attached PDF]

ATTACHMENT for ADDENDUM F

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.	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. Contractor will cooperate with EA and law enforcement to protect the integrity of investigations into the Breach as provided in the DPA.

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	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below. OR 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	PLEASE USE TEMPLATE BELOW.