



DATA SECURITY AND PRIVACY PLAN

WHEREAS, the Baldwinsville Central School District (hereinafter “School District”) and Blooket LLC (hereinafter “Contractor”) entered into an agreement dated October 12, 2023 (hereinafter “Agreement”) for Blooket LLC (hereinafter “Services”). The parties agree that such agreement shall consist of the Terms of Service for the purchase of Blooket.com for subscriptions purchased by the School District pursuant to an online purchase order or online purchase made by representatives from the School District with the authority to make such purchase.

WHEREAS, pursuant to the requires under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

1. During the term of the Agreement with the School District, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the School District’s Data Security and Privacy Policy in the following way(s): Contractor follow such laws. The School District has not provided a copy of the School District Data Security and Privacy Policy.

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement: Contractor encrypts data in motion and at rests. Contractor uses firewalls and passwords as administrative controls for the protection of data.

3. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the School District’s Parents Bill of Rights for Data Privacy and Security and will comply with same.

- a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.
- b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the “Supplemental Information” appended to the Agreement.

- c. At the end of the term of the Agreement, Contractor will destroy, and at the direction of the School District return, all student data and all teacher and principal data in accordance with the “Supplemental Information” appended to the Agreement.
- d. Student data and teacher and principal data will be stored in accordance with the “Supplemental Information” appended to the Agreement.
- e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided periodically by the In House Counsel for Contractor.

5. Subcontractors (check one):

Contractor shall not utilize sub-contractors.

XX Contractor shall utilize sub-contractors. Contractor shall manage the relationships and contracts with such sub-contractors in the following ways in order to ensure personally identifiable information is protected: Contractor shall enter into contractual agreement with specific data privacy protection provisions.

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information: *Contractor shall follow its data security plan.*

7. Termination of Agreement.

- a. Within 30 days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession, Contractor reserves the right to retain data for legal purposes. Contractor may retain any data which has been deidentified.; AND



- b. Within 30 days of termination of the Agreement and upon the written election to do so as described above, Contractor shall return all data to the School District using a method described in such notice; OR
Transition all data to a successor contractor designated by the School District in writing using a method described in such notice.

8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Contractor hereto has executed this Data Security and Privacy Plan as of October 13, 2023.

CONTRACTOR, Blooket LLC

By: Gregory D. Stewart
Title: Managing Member

SUPPLEMENTAL INFORMATION ADDENDUM
PARENTS BILL OF RIGHTS AND ADDITIONAL DATA PROTECTION MANDATES

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 Blooket LLC (the “Contractor”) are limited to the purposes authorized in the contract between the Contractor and Baldwinsville Central School District (the “School District”). The parties agree that such underlying contract between the parties shall be the Terms of Service of Blooket LLC for subscriptions purchased by the School District by parties with the express authority to enter into such contract. The term of the contract shall be determined by the subscription agreement.

2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor 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., FERPA; Education Law §2-d; 8 NYCRR Part 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 and upon notice to Contractor specifying the protected data which was shared with Contractor pursuant to the underlying agreement, protected data will be exported to the School District and/or destroyed by the Contractor 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 Family Educational Rights and Privacy Act (“FERPA”) stored by the School District in a Contractor’s product and/or 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 Contractor’s product and/or service 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 Contractor by the School District will be stored securely and encrypted both in transit and at rest. The measures that Contractor 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. The Vendor shall establish a data security and privacy plan which it will make available to the School District.

6. **ENCRYPTION PRACTICES:** The Contractor 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.

7. **NOTIFICATION OF BREACH:** Vendor shall promptly notify the School District of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach. The Vendor shall cooperate with the School District, educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.