**Nanuet Union Free School District**
**Vendor Agreement**

1. Notwithstanding any of the above, the parties agree that New York State Education Law sections 2-d, 101, 207 and 305 and its implementing regulations (Part 121) must be strictly adhered to by the software provider, its agents, officers, employees and third part contractors.

2. The software provider specifically incorporates into this agreement the District Bill of Privacy Rights attached to this agreement as Exhibit A and it agrees to fully abide by them. The additional information required for each agreement will also be included as an attached to the Bill of Rights.

3. In addition, the software provider agrees to the following as provided in 8 NYCRR 121:
   a. To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;
   b. To comply with the data security and privacy policy of the educational agency with whom it contracts, Education Law § 2-d, and 8 NYCRR 121;
   c. To limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
   d. To not use the personally identifiable information for any purpose not explicitly authorized in its contract;
   e. To not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i) except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or (ii) unless required by statute or court order and the third-party contractor provides 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. To maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
   g. To use encryption to protect personally identifiable information in its custody while in motion or at rest; and
   h. To 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. (b) Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

4. The software provider shall promptly notify each educational agency with which it has a

contract 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.

5. The software provider also acknowledges the accuracy of Appendix B to this agreement regarding its Data and Security Procedures.

6. The software provider must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

**Vendor Agreement – This Section To Be Completed By Vendor**

Bill of Rights Supplemental Information (to be filled out for each software/online package:
The supplemental information must be developed by the educational agency and include the following information:

(1) List 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;

We limit the data collected from students or children to only that which is necessary to meet the educational purposes of the tool. We do not collect sensitive data like biometric or health data or behavior data. We do not use student PII for commercial use. We do not disclose PII to third parties for non-educational commercial purposes.
Data is limited to: Name; School/account name email address of administrators or teachers; IP address and browser information; Status of users as administrator, teacher/student

2) Explain 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); 6

Student Records are records that are directly related to a student and maintained by FableVision on behalf of a school or district subscriber. Data is never disclosed externally except when provided for technical support. Student emails are not collected or used by the system and we do not communicate with students. Students can not interact with other students outside of the system. Teachers can not use the system to communicate with students.

(3) State 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 educational agency, and/or whether, when and how the data will be destroyed).

Student Records are records that are directly related to a student and maintained by FableVision Learning on behalf of a school or district subscriber. Data is never disclosed externally except when provided for technical support. Student emails are not collected or used by the system and we do not communicate with students. Students can not interact with other students outside of the system. Teachers can not use the system to communicate with students.

(4) State 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;

FableVision is used in schools at the direction of our customers. In addition, we are obligated under FERPA to remain under the direct control of our customers with respect to our use and maintenance of student personal information that is part of the education record. As such, if you use FabMaker Studio through a school account and wish to exercise your rights in respect to student personal information, please contact your education institution and we will work with them to facilitate your request.

All other users and visitors may exercise these rights by: Calling us at phone number: 1-800-828-0017; Emailing us at info@fablevisionlearning.com; Or mailing us at P.O. Box 1242 - Dedham, MA 02027

Your exercise of the above rights is subject to certain exemptions to safeguard the public interest and our interests. Requests to exercise these rights may be granted in whole, in part, or not at all, depending on the scope and nature of the request and applicable law. Where required by applicable law, we will notify you if and why we are unable to fulfill your request.

(5) State 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 and data security and privacy risks mitigated; and

Our servers are located in a secured, locked, and monitored environment to prevent unauthorized entry or theft, and

are protected by a firewall. The servers are located in a data center in the United States and backed up daily to a secure, U.S.-based, off-site data center.

(6) Explain how the data will be protected using encryption while in motion and at rest.
Our servers are located in a secured, locked, and monitored environment to prevent unauthorized entry or theft, and are protected by a firewall. The servers are located in a data center in the United States and backed up daily to a secure, U.S.-based, off-site data center.

**Data Security and Privacy**

(1) Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy; Our servers are located in a secured, locked, and monitored environment to prevent unauthorized entry or theft, and are protected by a firewall. The servers are located in a data center in the United States and backed up daily to a secure, U.S.-based, off-site data center.

(2) Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract; Our servers are located in a secured, locked, and monitored environment to prevent unauthorized entry or theft, and are protected by a firewall. The servers are located in a data center in the United States and backed up daily to a secure, U.S.-based, off-site data center.

(3) Demonstrate that it complies with the requirements of Section 121.3(c) of this Part (Bill of Rights); FableVision Learning Data Security & Privacy Plan, which covers the elements of 121.3, is provided on our website.
https://www.fablevisiongames.com/documents/March2023_FableVision_Data_PrivacyPolicy.pdf

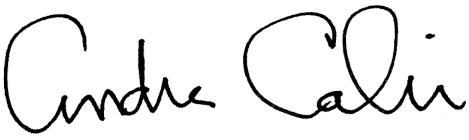
(4) Specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access; Minimal access is stored, and for pupils it is not linked to individuals that can be identified. Access to the database is limited to administrative and technical staff.

(5) Specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected; Minimal access is stored, and for pupils it is not linked to individuals that can be identified. Access to the database is limited to administrative and technical staff.

6) Specify how the third-party 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; In the event of unauthorized access to Personally Identifiable Information, we will notify the affected subscriber(s) in accordance with applicable law, and as appropriate, coordinate with the subscriber to support notification of affected individuals, students, and families.

(7) Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires. We store PII indefinitely, or until a request is put in to have this data deleted by a customer or at FableVision's discretion. School districts and administrators cannot delete student PII, but the FableVision systems team will do so upon written request.

Vendor: FableVision Learning/Reynolds Center

Signature: 

Date: Oct. 11, 2023