

Data Sharing and Confidentiality Agreement (Education Law 2-d Rider)

between the

ROCKY POINT UNION FREE SCHOOL DISTRICT

And

BOOK CREATOR/TOOLS FOR SCHOOLS, INC

1321 Upland Drive, Suite 8524 Houston, TX 77043

(Kami Limited/Notable Inc. provides Rocky Point students and staff resources related to document sharing, editing, and annotating.)

Supplemental Agreement dated this 17th Day of December between the ROCKY POINT UNION FREE SCHOOL DISTRICT (the “District”), located at 90 ROCKY POINT-YAPHANK ROAD, ROCKY POINT, NEW YORK, 11778, and Book Creator/Tools for Schools, Inc.. (the “Contractor”) are parties to a contract or other written agreement pursuant to which Contractor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”) from the District for purposes of providing certain products or services to the District.

WHEREAS, the District and the Vendor have entered into a contract (hereinafter the “Agreement”) whereby the Vendor may receive Student Data or Teacher or Principal Data, as those terms are defined in Education Law §2-d; and

WHEREAS, the Vendor represents that it will only share Protected Information with third party subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of the Vendor under this Contract and all applicable New York State and Federal laws.

WHEREAS, the District and the Vendor wish to enter into an Agreement in order to comply with Education Law §2-d the Vendor agrees that it will comply with all terms set forth in the Agreement. To the extent that any terms contained in the Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that the Vendor has online or written Privacy Policies or Terms of Service (collectively, “TOS”) that would otherwise be applicable to its customers or users of the products or services that are the subject of the Agreement between the District and Contractor to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

NOW THEREFORE, in consideration of the mutual promises below, the District and the Vendor agree as follows:

1. **Defined Terms:** Unless otherwise indicated below or elsewhere in this Supplemental Agreement, all capitalized terms shall have the meanings provided in Education Law §2-d.
 - a. “Educational Agency” shall generally have the same meaning as the term Educational Agency at Education Law §2-d(1)(c), and in reference to the party to this Agreement

shall mean the ROCKY POINT UNION FREE SCHOOL DISTRICT.

- b. “Third Party Subcontractor” shall mean any person or entity, other than an Educational Agency, that receives Student Data or Teacher or Principal Data from an Educational Agency pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs.
 - c. “Protected Data” means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Agreement.
 - d. “Student” means any person attending or seeking to enroll in an Educational Agency.
 - e. “Student Data” means Personally Identifiable Information of a “Student.”
 - f. “Eligible Student” means a Student who is eighteen years or older.
 - g. “Parent” means a parent, legal guardian, or personal in parental relation to a Student.
 - h. “Building Principal” or “Principal” means a building principal subject to annual performance evaluation review under Education Law §3012-c.
 - i. “Classroom Teacher” or “Teacher” means a teacher subject to annual performance evaluation review under Education Law §3012-c.
 - j. “Teacher or Principal Data” means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Agreement..
 - k. “Personally Identifiable Information” shall have the following meanings:
 - i. As applied to Student Data, shall mean Personally Identifiable Information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA)
 - ii. As applied to Teacher or Principal Data, shall mean Personally Identifiable Information as that term is defined in Education Law §3012c.
 - l. “NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).
2. The District has developed the **Parents’ Bill of Rights for Data Privacy and Security**, the terms of which are applicable to the Agreement between the District and the Vendor and are incorporated into this Supplemental Agreement. The Parents Bill of Rights for Data Privacy and Security states:
- a. A student's personally identifiable information cannot be sold or released for any commercial purposes.
 - b. Parents have the right to inspect and review the complete contents of their child's education record maintained by the Rocky Point Union Free School District.
 - c. State and federal laws protect the confidentiality of personally identifiable information. 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.

- d. A complete list of all student data elements collected by the State is available for public review at

<http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>

or a copy may be obtained by writing to:

Office of Information & Reporting Services
New York State Education Department, Room 863 EBA 89
Washington Avenue
Albany, NY 12234

- e. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Aaron Factor, Executive Director of Curriculum, Technology, & Innovation
Rocky Point UFSD
90 Rocky Point-Yaphank Road
Rocky Point, NY, 11778
631-849-7080 afactor@rockypoint.k12.ny.us

- f. “Supplemental information” for each contract into which the District enters with a third party who receives student data or teacher or principal data shall:

- i. The exclusive purposes for which the student data or teacher or principal data will be used;
 - ii. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
 - iii. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
 - iv. 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; and
 - v. 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, including whether such data will be encrypted.
- g. This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department’s Chief Privacy Officer, as well as emerging guidance documents.

3. As required by Education Law §2-d(3)(c), the District has developed the following “supplemental information” for the Agreement with the Vendor:

- a. Student Data and/or Teacher or Principal Data which the Vendor comes into possession as part of its Agreement with the District shall be used for the exclusive purpose(s) of performing Contractor’s obligations under this Agreement.
- b. The Vendor will ensure that any and all subcontractors, persons or entities that the Vendor may share the Student Data and/or Principal or Teacher Data with will abide by the terms of the Agreement, this Supplemental Agreement, and/or the

data protection and security requirements set forth in Education Law §2-d.

- c. When the Agreement terminates between the District and the Vendor, the Vendor shall return such data to the District or if agreed to by the District, destroy the remaining Student Data and/or Principal or Teacher Data that the Vendor still maintains in any form in a manner agreeable to the district.
- d. Any challenges concerning the accuracy of Student Data and/or Principal Data shall be handled directly between the District and the Parent, Student, Eligible Student, Teacher or Principal. The Vendor agrees to abide by the outcome of such challenges and make any corrections and/or changes to the applicable Student Data and/or Principal or Teacher Data as determined by the District.”
- e. The District and the Vendor hereby agree that the Student Data and/or Principal or Teacher Data shall be stored in the following manner:

[The Vendor to attach a detailed procedure in which Student Data and/or Principal or Teacher Data will be stored, and the security procedures that will be taken to ensure that the Data will be protected, and provide information on how the data will be encrypted.]

4. As required by Education Law §2-d(5)(e), the Vendor hereby agrees that any officers or employees of the Vendor, including any third-party subcontractors or assignees, who have access to Student Data or Teacher or Principal Data will have or will receive training on the Federal and New York State laws governing confidentiality of Student Data and/or Principal or Teacher Data prior to receiving access.

[The Vendor to attach a detailed document specifying how employees and its assignees receive or will receive training on the laws governing data prior to receiving access to the data. The Vendor should indicate in this document if they will use sub-contractors and how it will manage the subcontractor relationships and contracts.]

5. As required by Education Law §2-d(5)(f), the Vendor hereby agrees that it shall:
 - a. Limit internal access to education records to those individuals that are determined to have legitimate educational interests;
 - b. Not use the educational records for any other purposes than those explicitly authorized in the Agreement or this Supplemental Agreement;
 - c. Except for authorized representatives of the Vendor to the extent they are carrying out the Agreement or this Supplemental 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 a notice of the disclosure to the State Education Department, District 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 the statute or court order.
 - d. Maintain administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, and that align with the NIST Cybersecurity Framework 1.0;

- e. Store all data in the continental United States (CONUS) or Canada.
- f. Vendor will 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 U.S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2).

6. Breach and unauthorized release of Personally Identifiable Information:

- a. In accordance with Education Law §2-d(6), the Vendor shall be required to notify the District of any breach of security resulting in an unauthorized release of Student Data and/or Principal or Teacher Data by the Vendor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for Student Data Privacy and Security, the data privacy and security policies of the District and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. The District shall, upon notification by the Vendor, be required to report to the Chief Privacy Officer, who is appointed by the State Education Department, any such breach of security and unauthorized release of such data.
- b. In the case of an unauthorized release of Student Data, the District shall notify the Parent or Eligible Student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such Student in the most expedient way possible and without unreasonable delay. In the case of an unauthorized release of Teacher or Principal Data, the District shall notify each affected Teacher or Principal of the unauthorized release of data that includes Personally Identifiable Information from the Teacher or Principal's annual professional performance review in the most expedient way possible and without unreasonable delay.
- c. To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.
- d. In the case of notification to a Parent, Eligible Student, Teacher or Principal due to the unauthorized release of student data by the Vendor, or its subcontractors or assignees, the Vendor shall promptly reimburse the educational agency for the full cost of such notification, as required by Education Law §2-d(6)(c).

[Attach a document specifying how the Vendor will manage incidents including specifying any plans to identify incidents, and to notify the District.]

7. Miscellaneous:

- a. The District and Contractor agree that if applicable laws change and/or if the Commissioner of Education implements Regulations which affects the obligations of the parties herein, this Agreement shall be deemed to incorporate such changes as necessary in order for the District and the Vendor to operate in compliance with the amendment or modified requirements under the applicable laws or regulations.
- b. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the District to comply with the applicable laws or regulations.
- c. Nothing express or implied in this Agreement is intended to confer upon any person other than the District, Contractor and their respective successors and assigns any rights, remedies, obligations or liabilities.

- d. This agreement expires June 30, 2024. Upon expiration of this Contract without a successor agreement in place, the Vendor shall assist the Rocky Point Union Free School District in exporting all Protected Information previously received from, or then owned by the Rocky Point Union Free School District.
- e. Upon expiration of this Contract with a successor agreement in place, the Vendor will cooperate with the Rocky Point Union Free School District as necessary to transition protected data to the successor vendor prior to deletion. The Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of the Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of the Vendor in secure data center facilities.
- f. The Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by the Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement.

BY THE VENDOR: Book Creator/Tools for Schools Inc.

Thom Leggett

Name (Print)

T.W. Leggett

Signature

VP Engineering

Title

1/12/2022

Date

The text in bold is quoted directly from NY Education Law §2-d. The following text is an explanation of how Tools For Schools Inc meets or exceeds these requirements.

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 mission to empower the next generation of creators includes some important principles about how we safeguard the data you entrust to us.

We are COPPA, FERPA and GDPR compliant: Book Creator is fully compliant with these important laws and we're proud to have achieved COPPA and FERPA certification from the Internet Keep Safe Alliance.

Teachers are always in control: For example, a student's book is private by default. Only teachers can choose to share a book with a wider audience.

We don't sell user data or advertise: We will never advertise or sell data about you. Our business model is simple – we charge for access to Book Creator.

We protect your information: We use security industry best practices, such as encryption of your data in transit and at rest. All data is stored in Google Cloud offering the best security in the world.

Ownership of content: Your books belong to you, and you can download them at any time.

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;**

All employees are vetted for working with student data.

Regular security audit conducted (quarterly). This includes user access review, information security policy adherence and both static and dynamic application security scans.

Regular penetration tests conducted (at least annually).

Data is encrypted at-rest and in-transit using industry standard mechanisms - see <https://cloud.google.com/security/>

Access to systems that store, process or transmit data is controlled by a role-based access system. Users are authenticated by this system using a strong password and

two-factor authentication (not SMS-based).

Regular employee training (internally and by iKeepSafe) to ensure awareness of, and compliance with, COPPA, FERPA, GDPR, NY Education Law 2-d.

All data is stored in Google-owned datacenters in the continental US. Detailed information about the administrative, technical and organisational protections can be found here: <https://cloud.google.com/security/>.

The Book Creator terms and privacy policy can be found here: <https://bookcreator.com/privacy-policy/>

All data in flight sent using SSL/TLS. See <https://cloud.google.com/security/encryption-in-transit/> for more details.

Encryption at rest is AES 128/256 provided by Google Cloud: <https://cloud.google.com/security/encryption-at-rest/>.

3. **demonstrate that it complies with the requirements of Section 121.3(c) of this Part;**

Some information is included below to help the educational agency develop the supplemental information for the parents bill of rights for data privacy and security for Tools for Schools Inc.

1. **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 use student/teacher/principal data to:

- provide Book Creator and make sure you can use it properly and effectively;
 - manage and administer your account and the books that you create;
 - respond to any questions, requests or complaints we receive from you;
 - communicate with you about Book Creator if we need to;
 - investigate potential illegal activities on Book Creator;
 - analyse use of Book Creator; and
 - to improve Book Creator.
2. We will never use your information to target advertising at you based on your behavior. We will not build a personal profile of you other than for supporting authorised educational or school purposes, or as authorised by you (or by a parent or guardian if necessary). We also won't use your information for any purposes except those above without letting you know and getting your permission if necessary.

More information here: <https://bookcreator.com/pp-us/>.

- 3. 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);**

Any and all sub-contractors are engaged in such way as to preserve the same obligations and protections outlined in this plan.

- 4. 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).**

Upon termination or expiry of the contract, data can be destroyed on written request; or returned to the educational agency within 30 days of written request as JSON data and ePub 3.0 book files.

- 5. 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; including technical support;**

A teacher or principal may challenge the accuracy of the data by contacting our support team by visiting <https://support.bookcreator.com/> and selecting "Get support for Book Creator online".

Suewan Kemp, Support Operative

Mail: 1321 Upland Dr., Suite 8524, Houston, TX 77043.

Phone: 877-366-5116

A parent, student or eligible student may challenge the accuracy of the data by contacting the educational agency who will contact Tools for Schools on their behalf.

- 6. 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**

All data is stored in Google-owned datacenters in the continental US. Detailed information about the administrative, technical and organisational protections can be found here: <https://cloud.google.com/security/>.

The Book Creator terms and privacy policy can be found here: <https://bookcreator.com/privacy-policy/>

7. address how the data will be protected using encryption while in motion and at rest.

All data in flight sent using SSL/TLS. See <https://cloud.google.com/security/encryption-in-transit/> for more details.

Encryption at rest is AES 128/256 provided provided by Google Cloud: <https://cloud.google.com/security/encryption-at-rest/>.

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;

All employees who have access to student data are required to take annual training on their obligations under FERPA and COPPA as provided by iKeepSafe.

All employees who have access to student data are required to take annual training on their obligations under NY Education Law §2-d.

All employees who have access to student data are required to take annual training NIST Cybersecurity and Privacy Framework v1.1.

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;

Any and all sub-contractors are engaged in such way as to preserve the same obligations and protections outlined in this plan.

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;

[Incident Reporting Policy](#)

We maintain an operational Incident Reporting Policy - copy available on request.

- 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.**

Upon termination or expiry of the contract, data can be returned to the educational agency, ****within 30 days of a written request, as JSON data and ePub 3 book files.

We may transfer data to a successor contractor. We may transfer our rights and obligations under these terms to another organisation. We will contact you to let you know if we plan to do this. If you are unhappy with the transfer you may contact us to end the contract within 30 days of us telling you about it. More details are in Section 11 of our standard terms and conditions: <https://bookcreator.com/terms-of-service/>

Data is removed from servers using NIST compliant secure deletion. Certification of deletion available on written request.

Supplemental information

Data Protection Officer: Thom Leggett, thom@bookcreator.com

Main point of contact for service contract: David Swift, david@bookcreator.com

NIST Cyber Security Framework 1.1

Alignment with NIST CSF v1.1 Framework

(<https://www.nist.gov/cyberframework/new-framework>) is assured during our regular internal quarterly security audits.

Reference

The full legal text of NY 2-d for reference:

[part-121.pdf](#)