

**TEMPLATE AGREEMENT<sup>1</sup>**

**EAST RAMAPO CENTRAL SCHOOL DISTRICT**  
**DATA PRIVACY AGREEMENT**

**EAST RAMAPO CENTRAL SCHOOL DISTRICT**  
**and**

This Data Privacy Agreement ("DPA") is by and between the East Ramapo Central School District, ("EA"), an Educational Agency, and \_\_\_\_\_ ("Contractor"), collectively, the "Parties". This DPA is a rider to the Service Agreement dated \_\_\_\_\_ that governs the provision of \_\_\_\_\_ to the EA.

**ARTICLE I: DEFINITIONS**

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** Means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.

---

<sup>1</sup>This is a template agreement only, and its terms and conditions may be subject to change.

6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means student personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable student information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency 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.

## ARTICLE II: PRIVACY AND SECURITY OF PII

### 1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated \_\_\_\_\_ (the "Service Agreement"); Contractor may receive PII regulated by applicable New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part

99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

**2. Authorized Use.**

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

**3. Data Security and Privacy Plan.**

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

**4. EA's Data Security and Privacy Policy**

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

**5. Right of Review and Audit.**

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

**6. Contractor's Employees and Subcontractors.**

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and

the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any unauthorized party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

#### **7. Training.**

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

#### **8. Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

#### **9. Data Return and Destruction of Data.**

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA. Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA as prescribed in this Agreement. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) With regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any

and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

- (c) Upon request, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

**10. Commercial or Marketing Use Prohibition.**

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

**11. Encryption.**

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

**12. Breach.**

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified mail, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.
- (b) Notifications required under this paragraph must be provided to the EA at the following address:

Name: Bhavin Gandhi  
Title: Data Protection Officer  
Address: 105 S. Madison Avenue  
City, State, Zip: Spring Valley, NY 10977  
Email: [DPO@ercsd.org](mailto:DPO@ercsd.org)

### **13. Cooperation with Investigations.**

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach of data governed by this Agreement. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

### **14. Notification to Individuals.**

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

### **15. Termination.**

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

## **ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS**

### **1. Parent and Eligible Student Access.**

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

### **2. Bill of Rights for Data Privacy and Security.**

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.


**ARTICLE IV: MISCELLANEOUS**

**1. Priority of Agreements and Precedence.**

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

**2. Execution.**

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY	CONTRACTOR
BY: 	BY: <i>Jimmy Longley</i>
Bhavin Gandhi	
Director of Information Technology	
Date: 7-7-2021	Date:

**EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security**

The East Ramapo Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information in educational records from unauthorized access or disclosure in accordance with Education Law § 2-d, and all other applicable State and Federal laws.

The East Ramapo Central School District establishes the following Parents' Bill of Rights in which parents, legal guardians, persons in parental relationships, and/or Eligible Students, can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://www.nysed.gov/data-privacy-security/student-data-inventory) and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA to: Bhavin Gandhi, Data Protection Officer at [DPO@ercsd.org](mailto:DPO@ercsd.org) or 845-577-6081; (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-](http://www.nysed.gov/data-privacy-)



[security/report-improper-disclosure](#), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

<b>CONTRACTOR</b>	
<b>Signature</b>	
<b>Printed Name</b>	
<b>Title</b>	
<b>Date:</b>	

**EXHIBIT B**

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY  
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE  
PERSONALLY IDENTIFIABLE INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date Contract End Date
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>• Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.</li> <li>• Securely delete and destroy data.</li> </ul>
<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

<p><b>Secure Storage and Data Security</b></p>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p>  <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p>
<p><b>Encryption</b></p>	<p>Data will be encrypted while in motion and at rest.</p>

<p><b>CONTRACTOR</b></p>	
<p><b>Signature</b></p>	<p><i>Jimmy Longley</i></p>
<p><b>Printed Name</b></p>	
<p><b>Title</b></p>	
<p><b>Date:</b></p>	

**EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN**

**CONTRACTOR'S DATA PRIVACY AND SECURITY 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.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	
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.	

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.	
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the EA.	
8	Outline how your data security and privacy program/practices <b>align</b> with the EA's applicable policies.	
9	Outline how your data security and privacy program/practices <b>materially align</b> with the NIST CSF v1.1.  <a href="https://www.nist.gov/cyberframework/new-framework">https://www.nist.gov/cyberframework/new-framework</a>	

Revised: 6/29/21

# Data Security and Privacy at BookNook

In order to deliver a customized learning experience, BookNook needs to collect and handle private student data. We respect the sensitivity of this information and treat data security as a top priority.

BookNook implements practices covering the prevention, detection and response to security concerns that we regularly align with the [NIST Cybersecurity Framework](#). For additional information about BookNook's data practices, please refer to our [Privacy Policy](#) and [Terms of Use](#).

BookNook works with partnering LEAs to jointly ensure compliance with the Family Education Records Privacy Act of 1974 ("FERPA") regulations, and all other applicable federal, state, and local requirements to protect the confidentiality of educational records, provide eligible parties the opportunity to access and review such records, and limit further disclosure of personal information only as necessary to support the TEA educational purposes limited to the Agreement.

BookNook's tutors, using a tablet-based program, will assist students in 1-on-1 and small group reading and math intervention. Tutors provide both virtual and on-site structured instructional activities based on proven best practices for students in grades K-8. In order for BookNook to effectuate its service, BookNook requires the use of student data from partnering LEAs.

## Compliance with Family Educational Rights and Privacy Act

The data to be shared under this Agreement includes personally identifiable information ("PII") of students as defined under the Family Education Records Privacy Act of 1974 ("FERPA") (see 20 U.S.C. § 1232g). Disclosure is permitted because BookNook ("Recipient") is a contractor to whom the partnering LEA has outsourced institutional services or functions, such that it is "acting for" the partnering LEA and is (1) performing an institutional service or function for which the partnering LEAs would otherwise use employees; is (2) Is under the direct control of partnering LEAs with respect to the use and maintenance of education records; and (3) is subject to the requirements of 34 C.F.R. § 99.33(a) governing the use and redisclosure of personally identifiable information from education records in that BookNook hereby agrees that, except as permitted to do so by FERPA or its accompanying regulations, it will not disclose the personally identifiable information that it receives under this agreement and that is subject to FERPA to any other party without the prior consent of the parent or eligible student.

# Compliance with Children's Online Privacy Protection Act

To the extent BookNook shall be obtaining data directly from students under age 13, BookNook agrees to comply with any all applicable obligations (if applicable) of the Children's Online Privacy Protection Act (15 U.S.C. §§ 6501–6506).

## BookNook and LEA Responsibilities

### **BookNook agrees to:**

- (a) Provide the school and administration with any reasonably requested data and information on student attendance, activities, and performance with respect to BookNook's platform and services; and
- (b) Provide the school and administration with ongoing student progress data while using the BookNook platform and services.

### **Partnering LEAs agree to:**

- (a) Provide data on students participating in the program to BookNook for the purposes of enrolling students in the BookNook system, monitoring progress, and measuring outcomes;
- (b) Upon BookNook's reasonable request, provide BookNook with other student information such as parent contact information, demographic information, and qualitative information on academic performance;
- (c) Upon BookNook's reasonable request, provide BookNook with student reading achievement data from district-administered assessments.

## BookNook's Responsibilities

### **BookNook is responsible for:**

1. **Scope of Access.** BookNook shall obtain access to only those education records in which they have legitimate educational interests.
2. **Compliance.** All BookNook employees, contractors, and agents of any kind shall comply with all applicable provisions of this Agreement, FERPA and COPPA any other state or

federal laws with respect to the data shared under this Agreement. Nothing in this paragraph authorizes sharing data provided under this Agreement with any other entity for any purpose other than completing the BookNook's work under this Agreement.

3. **Storage.** BookNook shall maintain all data obtained pursuant to this Agreement in a secure computer environment and not copy, reproduce or transmit data obtained pursuant to this Agreement except as necessary to fulfill the purpose of the original request. All copies of data of any type, including any modifications or additions to data from any source that contains information regarding individual students, are subject to the provisions of this Agreement in the same manner as the original data. The ability to access or maintain data under this Agreement shall not under any circumstances transfer from the BookNook to any other institution or entity or unauthorized individual or agent. Data from partnering LEAs shall not be taken outside the United States.
4. **Publication.** BookNook shall not disclose any data obtained under this Agreement in a manner that could identify an individual student, except as authorized by FERPA, to any other entity. BookNook may publish results of general information (e.g., scope of participation), but specifically agrees to delete any data items that include personally identifiable student information, and to require all employees, contractors and agents of any kind to also abide by this paragraph.
5. **Data Transfer.** Data provided under this Agreement shall be transferred via a secure and private channel.
6. **Prohibited Disclosure.** BookNook shall not provide any data obtained under this Agreement to any party ineligible to receive data protected by FERPA or prohibited from receiving data from any entity by virtue of a finding under Sections 99.67(c), (d), or (e) of Title 34, Code of Federal Regulations.
7. **Destruction of Data.** BookNook shall destroy all personally-identifiable data within six (6) months if this Agreement is terminated for any reason.
8. **Assignment/Subcontractors.** BookNook shall not assign or subcontract this Agreement to any other entity without the express written consent of the partnering LEAs.
9. **Authorized Representative.** The Parties shall designate in writing a single authorized representative from each organization who will be able to send and request data under this Agreement. The authorized representatives shall be responsible for transmitting all data requests and maintaining a log or other record of all data requested and received pursuant to this Agreement, including confirmation of the completion of any projects and the return or destruction data as required by this Agreement. The partnering LEA or its agents may upon request review the records required to be kept under this section.



## Control over your data

BookNook only stores student data for the duration that it is necessary to fulfill our services for students. Information we collect on reading progress may be persisted for research purposes, but only after it is completely anonymized and all student PII is removed.

We will never sell or disclose student information without express permission, and data will be deleted or returned per any agreements with customers. We honor "right to forget" requests, and users can email [privacy@booknooklearning.com](mailto:privacy@booknooklearning.com) to retrieve or destroy their personal data.

## Data Retention and Destruction

When a license agreement is up for renewal, BookNook provides customers a 60 day grace period prior to scheduling data for removal. We provide these options to ensure we will be able to restore access to the data should there be a lapse in time between the contractual end date and the renewal processing.

Following the 60 day grace period, the data will be removed from Our primary data storage within 30 days and our backups within 90 days.

# Product security

## Role-based Access Controls

BookNook implements granular access control levels abiding by the principle of least privilege. Most users will not be able to access student PII unless it is needed.

Account passwords are salted and hashed using bcrypt, and login attempts are limited to protect from brute-force attacks.

## Responsible Disclosure

BookNook hosts an active bug bounty program to reward external security researchers for reporting vulnerabilities. Please direct inquiries to [security@booknooklearning.com](mailto:security@booknooklearning.com)

## Infrastructure Security

Our infrastructure security efforts focus on accelerating the pace of our engineering teams by providing the underlying tools, systems, processes, and knowledge resources to build secure and privacy-protecting systems.

All of BookNook's infrastructure runs in the cloud. Our primary cloud provider, AWS, conforms to security standards including SOC 1/SSAE 16/ISAE 3402, SOC 2, PCI DSS Level 1, ISO 27001, and FISMA. See <https://aws.amazon.com/compliance/> for more details.

## Vulnerability Detection

BookNook regularly updates our operating systems, language runtimes, and source libraries to the latest supported versions, and uses tooling to automatically detect and triage security issues in our downstream software dependency chain.

We regularly perform automated vulnerability scans to detect any issues or changes in our infrastructure.

## External Security Audits and Penetration Testing

BookNook works with an external provider to perform regular penetration testing every six months, and immediately triages and addresses any vulnerabilities discovered. We also work with independent third parties to perform security audits.

## Availability and Disaster Recovery

Our redundant, cloud-based architecture is designed to be highly available and resilient, and we maintain 99.9% uptime. See <https://status.booknooklearning.com/> for more details. Here, customers can opt in to receive prompt communication in the event of any service interruption.

BookNook leverages an API gateway to defend against automated Denial of Service (DoS) attacks against our infrastructure.

For disaster recovery purposes, BookNook regularly generates secure data backups via our cloud provider. These are automatically and securely deleted after no longer than 60 days.

## Data Encryption

All data maintained by the BookNook application is strongly encrypted at motion and while at rest. Our web application enforces TLS encryption for transmitted data, and all persisted information is protected by AES256 data encryption at rest.

## Data Isolation

Our software runs in a self-contained environment managed by our cloud provider. Processes, memory, file system, and network connections are strictly isolated and controlled. All BookNook data is maintained exclusively within the USA. See here for more information:

<https://www.heroku.com/policy/security>

## Secrets Management

Secret data such as passwords or API Keys that could grant access to student data are tightly protected at BookNook. Employees receive training to never share secrets via email, slack, text message, or similar platforms. All employees that must interface with student information are given access to a password manager tool and instructed to use it for sharing secrets and managing their passwords.

## Threat Detection

BookNook leverages automated secure logging, monitoring, and alerting tools to track and detect any unusual activity in the application.

## IT security

An effective security policy deals not just in code, but in people. Our IT security approach is designed to make it easy for BookNook employees to perform their jobs in a safe and transparent manner.

## Accounts

All employees that need to interact with student data are instructed to securely generate and store passphrases using a password manager that we provide.

BookNook defines strict policies for all accounts, such as email, enforcing 2-factor authorization and leveraging automated tooling to avoid phishing attacks.

When an employee leaves the company, all accounts are immediately deactivated and access to sensitive data is removed.

## Training

BookNook appreciates that our security starts with our staff, and provides regular training and resources to build a security-conscious culture.

BookNook maintains documentation on security practices, account permissions and data classifications, and access to sensitive information is limited to specifically trained staff.

## Background Checks

All BookNook employees with access to student PII undergo criminal background checks and sign agreements prohibiting the improper use or sharing of confidential information.

## Subcontractors

BookNook does not provide subcontractors access to confidential information without express written and public agreement. We isolate sensitive information from developer or testing environments, and take great care to anonymize data and prevent data leaking to subcontractors who need to interface with students.

## Incident Management and Response

BookNook documents a standard procedure for responding to security incidents. When a data breach is suspected, we will quickly notify our security team and establish a central communication channel. After any security incident or service interruption, the BookNook team conducts a thorough post-mortem analysis to identify underlying root causes or follow up work.

In a scenario where BookNook believes that private customer data could have been accessed by an unauthorized entity, we will immediately take steps to isolate the environment and ensure that the attacker's access is removed from the systems in question. We will analyze the incident to identify the extent of the breach and determine what customers were affected.

We will notify affected customers as quickly as possible, in no greater than 48 hours from the breach being detected.

If you have any questions about BookNook's security program, please contact us at [security@booknooklearning.com](mailto:security@booknooklearning.com).