DATA PRIVACY AGREEMENT

Albany-Schoharie-Schenectady-Saratoga BOCES
and

This Data Privacy Agreement ("DPA") is by and between the Albany-Schoharie-Schenectady-Saratoga BOCES ("EA"), an Educational Agency, and ____ Beneficent Technology, Inc. _____ ("Contractor"), collectively, the “Parties”.

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.
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 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 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 effective when signed by both parties ("Service Agreement"); Contractor may receive PII regulated by several 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 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, or render un-identifiable 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 other party unless:

(i) The Contractor has received written permission from a parent or eligible student to whom the data pertains to beforehand; or

(ii) 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.

Contactor 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, and 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, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall delete or render un-identifiable PII, in a format agreed to by the Parties to the EA.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to delete or render un-identifiable all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, 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 or rendered un-identifiable 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 rendered un-identifiable 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) 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.

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) business 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, 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: KellyRose Yaeger, Esq.

Title: Data Protection Officer

Address: 900 Watervliet-Shaker Road

City, State, Zip: Albany, New York 12205

Email: dpo@neric.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. Any documented 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**
Signature: John T. Phelan Jr. 42061F0222B702222FCB20C108B07063 contractworks	Signature: DocuSigned by: Lisa Wadors Verne 53CB5E51E8684A2...
Name: **John T. Phelan Jr.**	Name: Lisa Wadors Verne
Title: **Board President**	Title: Vice President Programs
Date: **08/24/2023**	Date: July 5, 2023

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

PARENT BILL OF RIGHTS

Albany-Schoharie-Schenectady-Saratoga BOCES (Capital Region BOCES), in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' 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;
- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov/data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, (518) 464-5139, DPO@neric.org, Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that BOCES engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, (518)-464-5139, DPO@neric.org, 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on BOCES' website https://www.capitalregionboces.org/.

CONTRACTOR	
[Signature]	DocuSigned by: Lisa Wadors Verne 53CD5E54E8684A2...
[Printed Name]	Lisa Wadors Verne
[Title]	Vice President Programs
Date:	July 5, 2023

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).

Name of Contractor	Beneficent Technology, Inc.
Description of the purpose(s) for which Contractor will receive/access PII	Providing accessible electronic materials to students with qualifying disabilities through Contractor's Bookshare service.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	This contract expires on June 30, 2024; and, shall automatically renew for four sequential one- year renewal periods unless terminated by either party upon 30 days prior written notice.
Subcontractor Written Agreement Requirement	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) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely dispose of or render un-identifiable data**.**

Challenges to Data Accuracy	Parents can challenge the accuracy of their student's data stored in Contractor's Bookshare service by following EA's procedure for requesting the amendment of education records under the Family Educational Rights and Privacy Act (FERPA). EA staff have direct access to correct or update data within District's Bookshare account(s) and they may also contact Contractor by email at support@bookshare.org if they need further assistance in correcting data.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Student Data provided to Contractor by EA will be stored in Amazon Web Services onservers located in the United States.
Encryption	Contractor certifies that encryption of Protected Data is applied in accordance with New York State Education Law Section 2-d 5(f)(5).

CONTRACTOR	
[Signature]	DocuSigned by: Lisa Wadors Verne 53CB5E51E8684A2...
[Printed Name]	Lisa Wadors Verne
[Title]	Vice President Programs
Date:	July 5, 2023

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**. 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.	To ensure Contractor's obligations under this Contract, Contractor conducts regular security scans, encrypts all data in transit and at rest, implements data and network segmentation to minimize data accessibility, and restricts data access exclusively to authorized employees. Contractor does not copy, reproduce, or transmit Student Data to any third party. The Contractor may send aggregated, anonymized data as necessary to fulfill the purpose of data requests by EA or by the U.S. Department of Education under the Cooperative Agreement that funds Bookshare.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	While Contractor's cybersecurity framework is not designed in accordance with any one particular established set of specifications, it is custom designed by Bookshare's engineering team in accordance with industry standard best practices with respect to protected data storage, privacy. including, but not limited to encryption, firewalls, passwords, protection of off-site records, and

		limitations of access to stored protected data to authorized staff. Please see Appendix A attached to this Exhibit C for greater details.
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.	The Contractor provides periodic data privacy and security training to employees who operate or regularly access systems that store Student Data. Further, Contractor shall provide the EA with contact information of an employee who the EA may contact if there are any security concerns or questions.
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.	All Benetech employees are required to sign a confidentiality agreement with Benetech as part of the onboarding process. Each Employee's obligation to preserve confidentiality extends to all third party, confidential information.
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.	In the event that Student Data is accessed or obtained by an unauthorized individual, Benetech shall provide notification to the affected Organization (such as a District or School) or the Individual Member without unreasonable delay, but not more than seven days after discovery of the incident. Benetech shall take the following steps: 1. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information

		may be provided as a supplement to the notice. 2. The security breach notification described above in section 1(a) shall include, at a minimum, the following information: - The name and contact information of the reporting District or School subject to this section. - A list of the types of personal information that were or are reasonably believed to have been the subject of a breach. - If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice. - Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided. - A general description of the breach incident, if that information is possible to determine at the time the notice is provided. 3. At Benetech's discretion, the security breach notification may also include any of the following: - Information about what Benetech has done to protect individuals

		whose information has been breached. - Advice on steps that the person whose information has been breached may take to protect himself or herself.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon receipt of a request from the EA, Contractor shall dispose of, or render un-identifiable, all Student Data obtained under the Data Privacy Agreement when it is no longer needed for the purpose for which it was obtained.
7	Describe your secure destruction practices and how certification will be provided to the EA.	In Contractor's history we have never been asked to delete student data. However, if we were to receive such a request, our subprocessor AWS would handle such destruction processes. Upon receipt of a request from the EA for deletion of student data, the Contractor will request that such data be deleted or rendered unidentifiable.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor regularly reviews our information collection, storage and processing practices, including physical security measures, to prevent unauthorized access to our systems. Contractor conducts application security testing, penetration testing, risk assessments, and continuous monitoring to ensure compliance with security policies. When you enter any information on the Bookshare Service, we encrypt the transmission of that information using Hypertext Transfer Protocol Secure (HTTPS) by default.

		Contractors database where we store PII is encrypted at rest. Contractor ensures passwords are stored securely using encryption. The Bookshare Service and associated services are hosted by third-party subprocessors in separate facilities. Contractor has established contractual agreements with these subprocessors to enforce enhanced security measures for safeguarding your data. Access to PII is limited to authorized Benetech employees, agents, or independent contractors who require the information to perform necessary processing on our behalf. These individuals are bound by stringent confidentiality obligations and may face disciplinary action or termination if they fail

APPENDIX A
to Exhibit C

Data Security
The security of PII is important to us. In order to ensure the security and integrity of the PII we collect, we have implemented a range of physical, technical, and administrative measures to prevent unauthorized access, disclosure, or misuse, and to maintain data accuracy. In particular:

- We regularly review our information collection, storage and processing practices, including physical security measures, to prevent unauthorized access to our systems.
- We conduct application security testing, penetration testing, risk assessments, and continuous monitoring to ensure compliance with security policies.
- When you enter any information on the Bookshare Service, we encrypt the transmission of that information using Hypertext Transfer Protocol Secure (HTTPS) by default.
- At Benetech, the database where we store your PII is encrypted at rest.
- We ensure passwords are stored securely using encryption.
- The Bookshare Service and associated services are hosted by third-party subprocessors in separate facilities. We have established contractual agreements with these subprocessors to enforce enhanced security measures for safeguarding your data.
- Access to PII is limited to authorized Benetech employees, agents, or independent contractors who require the information to perform necessary processing on our behalf. These individuals are bound by stringent confidentiality obligations and may face disciplinary action or termination if they fail to meet these obligations.

In the event of a security breach, we will make every effort to notify you electronically (subject to any applicable laws and reporting requirements) to allow you to take necessary precautions. Depending on your jurisdiction, you may have a legal right to receive written notice of a security breach.

Student Data Collection
PII is not a pre-requisite in the provision of, or a student's access to, or use of, the Bookshare service. Although the Bookshare platform does not require actual PII, the platform will process user name, age, grade, and disability type (whether or not such information is actual PII or "alias" data (known only to the school).

There are clearly some personal details that Bookshare considers useful in providing Bookshare services. It is important (i) that any student who abuses the Bookshare service (e.g., shares a book with anyone who is not a qualified print-disabled user) can be contacted and disciplined, if necessary, by the school or school district. Thus, to proceed using alias information, the school or school district must maintain a database in which the student's real name is paired with a random, unidentifiable, or coded user name and a valid password of each student accessing Bookshare and (ii) that it is noted when students have Individual Education Plans (IEPs) so they can be given access to educational materials from the National Instructional Materials Access Center (NIMAC.) These materials are only available to students with IEPs.
Anonymized and aggregated data on age, grade, disability type, IEP and/or 504 plans may be provided to fulfill the purpose of data requests by an education entity or by the U.S. Department of Education under the Cooperative Agreement that fully funds Bookshare.

Data Retention
We retain PII for as long as necessary to provide products and services to you and others, as described in the preceding description. PII associated with your account will be retained until your account is deleted, unless the data is no longer needed to provide the products and services.

Please note that that certain information may be retained even after your account is closed. This is done to comply with legal obligations, safeguard the security and well-being of our community and services, and prevent any misuse of our Terms. You have the option to delete your account whenever you wish.

Student Data Protection Policy
We do not retain students' PII beyond what is necessary for educational purposes, legal obligations, or to provide the services for which we receive or collect such information. In addition, students' PII is retained only for as long as their student account remains active, unless retention is required by law, by the student's school, or is necessary to ensure the safety of our community, our services, or to enforce our Term.