Data Privacy Agreement
State of New York

I. Scope
Beneficent Technology, Inc. (hereinafter "Vendor") is a non-profit organization who is providing access to its digital accessible book library service, known as Bookshare, to _____ (hereinafter "District") at no charge and in accordance with a pre-existing cooperative agreement ("Cooperative Agreement") between Vendor and the federal Department of Education, thereby making this agreement subject to the provisions and oversight provided by the U.S. Department of Education under the Cooperative Agreement. In recognition of the fact that Vendor has been engaged to provide access to Bookshare, it is understood as follows:

II. Vendor Status
Vendor acknowledges that for purposes of New York State Education Law §2-d it is a third-party contractor. As defined in New York State Education Law §2-d, Student Data, or Teacher or Principal Data shall be hereinafter referred to as "Protected Data." For any Protected Data that constitutes education records under the Family Educational Rights and Privacy Act (FERPA), Vendor shall be considered a school official with a legitimate educational interest in the educational records.

III. Confidentiality

Vendor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law §2-d and the terms set forth below.

IV. Use of Protected Data & Security Requirements

Vendor shall:

1. Limit internal access to Protected Data to those individuals that are determined to have legitimate educational interests.

2. Not use the Protected Data for any other purposes than providing access to Bookshare and those explicitly authorized in this Data Privacy Agreement.

3. Except for authorized representatives of Vendor to the extent they are carrying out the contract and for data requests from the U.S. Department of Education under the Cooperative Agreement, not disclose any Protected Data to any other party:

    a. Without the prior written consent of the parent or eligible student; or

    b. Unless required by statute or court order and the party provides a notice of the disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed,

unless providing notice of the disclosure is expressly prohibited by the statute or court order;

4. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Protected Data in its custody.

5. Use encryption technology to protect Protected Data while in motion or in its custody from unauthorized disclosure using a technology or methodology as specified by, or reasonably similar to, the secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

6. Ensure that Protected Data shall not be sold or used for marketing purposes.

7. Use industry standards, including the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework, with respect to Protected Data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored Protected Data to authorized staff.

8. Notify District of any breach of security resulting in an unauthorized release of Protected Data by it or its subcontractors and/or assignees in violation of applicable State or federal law, the Parents' Bill of Rights for Data Privacy and Security ("Bill of Rights") , the data privacy and security policies of District, and/or its obligations under this Data Privacy Agreement relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven (7) calendar days after the discovery of such breach.

   a. With approval of District, Vendor will notify affected students or staff of District whose personally identified data is reasonably believed to have been affected by an unauthorized release of such data due to a breach of security. Such notification shall be provided without unreasonable delay and in any case, no later than 30 days after the unauthorized release of data has been confirmed by Vendor.

   b. Where a breach or unauthorized release is attributed to Vendor, the Vendor shall pay for or promptly reimburse the District for the full cost of such notification.

9. Ensure that the subcontractors, persons or entities that Vendor will share the Protected Data with, if any, will abide by contractual obligations with respect to Protected Data set forth herein, including, but not limited to, the data protection and security requirements.

10. When the contract expires, Protected Data will, upon the written request of the District, be deleted by Vendor, as soon as reasonably possible and within no more than 30 days from the date of the request.

Data Security and Privacy Plan
Supplemental Information Regarding Third-Party Contractors

Vendor: <u>Beneficent Technology, Inc.</u>   Product: <u>Bookshare</u>

Collects: ☒ Student   ☒ Teacher or Principal Data   ☐ Does not collect

.

Part 1: Exclusive Purposes for Data Use
Please list the exclusive purposes for which the Protected Data will be used by Vendor: *Providing accessible electronic materials to students with qualifying disabilities through Vendor's Bookshare service*

Part 2: Subcontractor Oversight Details – Select the appropriate option below.
☐ This contract has no subcontractors. ☒ This contract has subcontractors. As such, Vendor will take the following steps to ensure that any subcontractors, assignees, or other agents who see, or receive, this protected data are contractually required to obey the same data protection and security requirements that the third-party contractor is required to obey under state and federal law: *Subcontractors agree to abide by data protection and security agreements as part of their contract with Vendor*

Part 3: Contract Lifecycle Practices
The contract expires on *July 31, 2025* unless renewed or automatically extended for a term pursuant to the agreement. When the contract expires, Protected Data will be: *deleted within 30 days*

Part 4: Data Accuracy / Correction Practices
. Parent [student, eligible student, teacher or principal] may challenge the accuracy . of the data by: *Parents can challenge the accuracy of their student's data stored in Vendor's Bookshare service by following District's procedure for requesting the amendment of education records under the Family Educational Rights and Privacy Act (FERPA). District staff have direct access to correct or update data within District's Bookshare account(s) and they may also contact Vendor by email at support@bookshare.org if they need further assistance in correcting data.*

Part 5: Security Practices
A. Protected Data provided to Vendor will be stored: (include *where* and *how*): *Protected Data provided to Vendor by District will be stored in Amazon Web Services on servers located in the United States*   B. The security protections taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry practices include: *Protected Data provided to Vendor by District is protected by commercially reasonable practices that include encryption, firewalls, and password protection*

Part 6: Encryption Practices
☒ By checking this box, Vendor certifies that encryption of Protected Data is applied in accordance with New York State Education Law Section 2-d 5(f)(5).

Part 7: Training Practices
☒ By checking this box, Vendor certifies that annual training on federal and state law governing confidentiality is provided for all officers, employees, or assignees who have access to Protected Data

Parents' Bill of Rights for Data Privacy and Security

District is committed to protecting the privacy and security for student, teacher and principal data. In accordance with New York Education Law § 2-d, District wishes to inform the community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Student data will be collected and disclosed only as necessary to achieve educational purposes in accordance with state and federal law.

3. Parents have the right to inspect and review the complete contents of their child's education record.

4. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

5. A complete list of all student data elements collected by the State is available for public review at: http://www.nysed.gov/data-privacysecurity/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

6. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at: http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure.

7. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third-party contractors are required by law to notify District within seven (7) days of discovery of the breach or unauthorized disclosure.

8. If District enters into a contract with a third-party in which student, teacher, or principal data is shared with a third-party, supplemental information for each such contract will be appended to this Parents' Bill of Rights.

9. Parents may access the State Education Department's Parents' Bill of Rights at: http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/parents-bill-of-rights.pdf

By signing below, Vendor agrees to abide by the terms and conditions set forth above.

_____
Signature

Date: _____

Vendor Signer Name (Printed):

Vendor Signer Title: