

STUDENT DATA PRIVACY AGREEMENT

Harrison Central Schools

(hereinafter referred to as “LEA”)

and

BENEFICENT TECHNOLOGY, INC.

This Student Data Privacy Agreement (“DPA”) is entered into by and between LEA and Beneficent Technology, Inc. (hereinafter referred to as “Provider”), together the “Parties” and each a “Party,” on the effective date set forth on the signature page. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, Provider has agreed to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) as described in Article I and Exhibit “A”; and

WHEREAS, Provider, by signing this Agreement, agrees to allow LEA to offer school districts in the same state the opportunity to accept and enjoy the benefits of the DPA for the Services described; and

WHEREAS, in order to provide the Services described in Exhibit “A,” the Provider may receive and LEA may provide documents or data that are covered by several federal and state statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

WHEREAS, Provider is a non-profit organization who is providing the Services to LEA at no charge and in accordance with a pre-existing cooperative agreement (“Cooperative Agreement”) between Provider and the federal Department of Education, thereby making this DPA subject to the provisions and oversight provided by the U.S. Department of Education under the Cooperative Agreement; and

WHEREAS, the documents and data transferred from LEA are also subject to applicable state student privacy laws (“State Privacy Laws”).

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

NOW THEREFORE, for good and valuable consideration, the Parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit “C”) transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with applicable privacy statutes, including but not limited to the FERPA, PPRA, COPPA, IDEA and State Privacy Laws. In performing these services, Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by LEA. Provider shall be under the direct control and supervision of LEA, and shall provide Services at LEA’s direction and request. Control duties are set forth below.
2. **Nature of Services Provided.** Provider agrees to provide the following digital educational services described in Exhibit “A.”
3. **Student Data to Be Provided.** In order for Provider to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit “B.”

- 4. DPA Definitions.** The definition of terms used in this DPA is found in Exhibit "C." In the event of a conflict, definitions used in this DPA shall prevail over other agreements including the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

- 1. Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of LEA. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per the Service Agreement shall remain the exclusive property of LEA. For the purposes of FERPA, Provider shall be considered a School Official, under the control and direction of LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer Pupil Generated Content to a separate account, according to the procedures set forth below.
- 2. Parent Access.** Provider and the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the Pupil's Records, correct erroneous information, and procedures for the transfer of Pupil Generated Content to a personal account, consistent with the functionality of Services. Provider shall respond in a reasonably timely manner to LEA's request for Personally Identifiable Information in a Pupil's Records held by Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, Provider shall refer the parent or individual to LEA, who will follow the necessary and proper procedures regarding the requested information.
- 3. Separate Account.** Provider shall, at the request of LEA, transfer Pupil Generated Content to a separate student account.
- 4. Third Party Request.** Except for data requests from law enforcement or government agencies such as the U.S. Department of Education under the Cooperative Agreement that include reporting obligations and/or audit requirements directed to Provider, should a different Third Party contact Provider with a request for data held by Provider pursuant to the Services, Provider shall redirect the Third Party to request the data directly from LEA. Provider shall notify LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.
- 5. No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement and/or otherwise authorized in this DPA and/or under the statutes referenced in this DPA.
- 6. Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to be bound by the terms of this DPA.
- 7. Separate Agreements with Students/Parents/Guardians.** Provider may offer individual accounts for access to the Bookshare services directly to American students with qualifying disabilities. For minor students, the signature of a parent or guardian is required. These separate accounts are not included in or governed by the terms of the Service Agreement or this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws.** LEA shall provide data for the purposes of the Service Agreement in compliance with applicable privacy laws including FERPA, PPRA, COPPA, IDEA, and State Privacy Laws.
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.
4. **District Representative.** At request of Provider, LEA shall designate an employee or agent of the District as the District representative for the coordination and fulfillment of the duties of this DPA.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** Provider shall comply with applicable state and federal laws and regulations pertaining to data privacy and security, including but not limited to FERPA, PPRA, COPPA, IDEA, and State Privacy Laws.
2. **Authorized Use.** Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services described in Exhibit A or as stated in the Service Agreement and/or otherwise authorized in this DPA including under the statutes referred to in subsection (1), above.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider shall not disclose any data obtained under the Service Agreement in a manner that could identify an individual student to any entity other than the U.S. Department of Education pursuant to the Cooperative Agreement in published results of studies as authorized by the Service Agreement. De-identified information, as defined in Exhibit "C," may be used by Provider in any way including for the purposes of development and improvement of educational sites, services, or applications.
5. **Disposition of Data.** Provider shall dispose of, or render as De-Identifiable Information, all Personally Identifiable Information obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain Personally Identifiable Information obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. LEA may request email notification confirming that the Personally Identifiable Information has

been disposed, email requests to be sent to: privacy@benetech.org. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate student account, pursuant to the other terms of the DPA. Nothing in the Service Agreement authorizes Provider to maintain Personally Identifiable Information beyond the time period reasonably needed to complete the disposition.

6. **Advertising Prohibition.** Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; or (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes, or offering individual Provider related accounts to students, families, or guardians.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** Provider agrees to abide by and maintain adequate data security measures to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in in Exhibit "D" hereto. These measures shall include, but are not limited to:
- a. **Passwords and Employee Access.** Provider shall make commercially reasonable efforts to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Data shall pass criminal background checks.
 - b. **Destruction of Data.** Provider shall dispose of, disposal as defined in Article IV, Section 5, all Personally Identifiable Information obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.
 - c. **Security Protocols.** Both Parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by Parties legally allowed to do so. Provider shall maintain all Student Data obtained or generated pursuant to the Service Agreement in a secure computer environment, which may include secure cloud based storage, and not copy, reproduce, or transmit Student Data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA under this DPA or by the U.S. Department of Education under the Cooperative Agreement.
 - d. **Employee Training.** Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide

LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

- e. **Security Technology.** The service shall use Secure Socket Layer (“SSL”), or equivalent technology to protect data from unauthorized access. The service security measures shall include server authentication and data. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
 - f. **Security Coordinator.** Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.
 - g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to be bound to the same requirements and duties as set forth in the terms of this Article V.
2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within five business days of the discovery of the incident. Provider shall follow the following process:
- a. 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.
 - b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. 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.
 - iv. 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.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - c. At LEA's discretion, the security breach notification may also include any of the following:
 - i. Information about what the agency has done to protect individuals whose information has been breached.

- ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. Provider agrees to adhere to requirements in applicable state and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- e. At the request and with the assistance of the LEA, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms ("General Offer"), (attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the Acceptance on said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. Provider shall be bound by this DPA for the duration of the Service Agreement or so long as Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.
2. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.
3. **Effect of Termination Survival**. If the Service Agreement is terminated, Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).
4. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with applicable privacy protections, including those found in FERPA, PPRa, COPPA, IDEA, and State Privacy Laws. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery or first class mail, postage prepaid, with a courtesy copy by email sent to the addresses set forth on the signature page.
6. **Application of Agreement to Other Agencies**. Provider may agree by signing the General Offer of Privacy Terms to be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.
7. **Entire Agreement**. This DPA constitutes the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties.

Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

8. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
9. **Governing Law; Venue and Jurisdiction**. This DPA will be governed and construed in accordance with the laws of the state in which LEA is located, without regard to the conflict of law principles. The Parties agree that any dispute, claim or controversy arising out of or relating to this Agreement, shall be settled by binding arbitration in accordance with the commercial arbitration rules of the American Arbitration Association, and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction, which court shall be an appropriate State or Federal Court in the county in which LEA is located. Arbitration shall be conducted virtually in accordance with the American Arbitration Association's Virtual Hearings offerings. Note that there is no judge or jury in an arbitration proceeding and the decision of the arbitrator shall be binding upon both Parties.

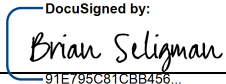
SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties have executed this Student Data Privacy Agreement as of the last day noted below.

LEA: Harrison Central Schools

Address: 50 Union Ave. Harrison NY 10528

Email Address: seligmanb@harrisoncsd.org

By:  _____
91E795C81CBB456...

Date 2/18/2022

Printed Name: Brian Seligman

Title/Position: CIO, Director of Technology

BENEFACTANT TECHNOLOGY, INC.

Address: 480 California Ave., Suite 201, Palo Alto, CA 94306-1609

Email Address: privacy@benetech.org

By: _____

Date _____

Printed Name: _____

Title/Position: _____

EXHIBIT "A"

DESCRIPTION OF SERVICES

Bookshare is an accessible online library for individuals with qualifying disabilities. Literary, musical, and theatrical works are provided in specialized, accessible digital formats exclusively for use by persons with qualifying disabilities.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data - Please specify:	

Category of Data	Elements	Check if used by your system
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT "C"
DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, Student Data, metadata, and user or Pupil-Generated Content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First and Last Name	Home Address
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Pupil Records.

Pupil Generated Content: Means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

Service Agreement: Refers to the Bookshare Organizational Agreement which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the

agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to CFR 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data as specified in Exhibit B is confirmed to be collected or processed by Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means an entity that is not a Party to this Agreement or a representative of a Party, Provider, LEA, or the U.S. Department of Education.

EXHIBIT "D"

ADDITIONAL DATA SECURITY REQUIREMENTS

Please contact us at privacy@benetech.org if you require additional data security requirements. We will review such additional requirements and create an addendum to this agreement, if we are able to agree to the additional requirements.

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and LEA and with an effective date set forth on the signature page to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to Provider to suit the unique needs of that LEA. Provider may withdraw the General Offer at its sole discretion.

BENEFCIENT TECHNOLOGY, INC.

BY: _____

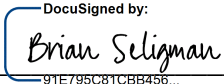
Date: _____

Printed Name: _____

Title/Position: _____

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and Provider shall therefore be bound by the same terms of this DPA.

BY:  _____
91E795C81CBB456...

Date: 2/18/2022

Printed Name: Brian Seligman

Title/Position cto, director of technology