EXHIBIT D

Data Sharing and Confidentiality Agreement

INCLUDING

PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

AND

SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Instructional Technology Free Application RFP response ("RFP") to which it is attached, to ensure that the RFP conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the RFP that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the RFP, or any terms contained within any other Exhibits attached to and made a part of the RFP response, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the RFP, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the RFP will have the same definition as contained within the RFP.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the RFP.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the RFP.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services through a Cooperative Educational Services Agreement with a BOCES, and as a result is able to use Vendor's Product pursuant to the terms of the RFP. The term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the RFP to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the RFP may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy. Erie 1 BOCES will provide Vendor with a copy of its policy and Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the RFP, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the RFP: Data Security and Privacy Plan included as Appendix 7

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the RFP" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor __x___will _____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the RFP. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the RFP, it will require such subcontractors, assignees, or other

authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the RFP," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the RFP is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the RFP and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the RFP.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the RFP, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the RFP," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

ERIE 1 BOCES

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES 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) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and 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.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the 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 the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

LC Franks

Signature

Lainey Franks

Printed Name

VP of Partnerships

Title

3/17/2022

Date

EXHIBIT D (CONTINUED)

Erie 1 BOCES has entered into an RFP with Tools for Schools Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

Book Creator Free Edition

Pursuant to the RFP response, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the RFP. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the RFP (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the RFP and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: any and all sub-contractors are engaged in such a way as to preserve the same obligations and protections outlined in this plan.

Duration of the RFP and Protected Data Upon Expiration:

The RFP commences on [date] and expires on June 30, 2024.

Upon expiration of the RFP without renewal, or upon termination of the RFP prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to

whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

In the event the RFP is assigned to a successor Vendor (to the extent authorized by the RFP agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.

Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

Appendix 7 Data Privacy and Security Plan

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

1. **Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;**

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

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

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

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

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

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

2. **specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;**

All employees are vetted for working with student data.

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

Regular penetration tests conducted (at least annually).

Data is encrypted at-rest and in-transit using industry standard mechanisms.

https://cloud.google.com/security/

Access to systems that store, process or transmit data is controlled by a role-based access system. Users are authenticated by this system using a strong password (following this advice: https://support.google.com/accounts/answer/32040?hl=en) and two-factor authentication (not SMS-based).

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

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

Some information in included below to help the educational agency develop the supplemental information for the parents bill of rights for data privacy and

security for Tools for Schools Inc.

1. **the exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;**

   We use student/teacher/principal data to:

   - provide Book Creator and make sure you can use it properly and effectively;
   - manage and administer your account and the books that you create;
   - respond to any questions, requests or complaints we receive from you;
   - communicate with you about Book Creator if we need to;
   - investigate potential illegal activities on Book Creator;
   - analyse use of Book Creator; and
   - to improve Book Creator.

2. We will never use your information to target advertising at you based on your behavior. We will not build a personal profile of you other than for supporting authorised educational or school purposes, or as authorised by you (or by a parent or guardian if necessary). We also won't use your information for any purposes except those above without letting you know and getting your permission if necessary.

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

3. **how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data,**

if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);

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

4. **the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).**

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

5. **if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;**

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

Suewan Kemp, Support Operative

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

Phone: 877-366-5116

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

6. **where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and**

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

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

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

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

Encryption at rest provided by Google Cloud: https://cloud.google.com/security/encryption-at-rest/.

4. **specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;**

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

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

5. **specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;**

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

6. **specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;**

   Incident Reporting Policy

7. **describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.**

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

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

Supplemental information

NIST Cyber Security Framework 1.1

Alignment with NIST CSF v1.1 Framework (https://www.nist.gov/cyberframework/new-framework) is assured during our regular quarterly security audits.