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 Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA 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 MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, 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 MLSA, 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 MLSA will have the same definition as contained within the MLSA.

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 MLSA.

(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 MLSA.

(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 and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA 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 MLSA 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. 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 MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: Tynker Additional Terms of Use for Educational Institutions

Effective Date: Feb 21, 2023

These Additional Terms of Use for Educational Institutions (the "Additional Terms") apply to all schools, school districts, and related entities and organizations, including but not limited to administrators, instructors, and professors who access or use the Services on their behalf (each an "Educational Institution"). For purposes of these Additional Terms, "you" shall mean an Educational Institution. These Additional Terms supplement (and do not supersede) our Terms of Use; however, in the event of a direct conflict, these Additional Terms shall prevail. Capitalized terms that are not defined below have the definitions given them in Tynker's Terms of Use.

I. General

1. Both parties agree to uphold their responsibilities under the Family Educational Rights and Privacy Act ("FERPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Children's Online Privacy and Protection Act ("COPPA"). We provide the Services as an outsourced institutional function under FERPA 34 CFR Part 99.31(a)(1). We recommend that all Educational Instructions provide appropriate disclosures to parents (including legal guardians and Eligible Students (as defined in FERPA), collectively "Parents") regarding your use of Tynker's Services and that you provide a copy of our Privacy Policy to Parents.
2. As between an Educational Instruction and Tynker, Education Records (as defined below) continue to be the property of and under the control of the Educational Instruction. You own all right, title and interest to and are solely responsible for all Education Records. Education Records shall mean student educational records that are: (1) directly related to your student; and (2) maintained by you or by a party acting for you ("Education Records"). We do not own, control, or license such Education Records, except as permitted under these Additional Terms and Tynker's Terms of Use and Privacy Policy.

II. Compliance with Family Educational Rights and Privacy Act - FERPA

1. FERPA requires that Educational Institutions keep personally identifiable information (as defined in FERPA, "PII") from Education Records confidential and cannot disclose them to a provider unless: (i) an Educational Institution has first obtained written consent from the Parents; or (ii) the disclosure of information falls into one of the exceptions provided for in the FERPA. One of the exceptions is releasing PII from Education Records to a school official with a legitimate educational interest. According to FERPA, teachers, contractors, consultants, volunteers, or other parties to whom the Educational Institution has outsourced institutional services or functions may be considered a school official. Furthermore, if these school officials need PII from Education Records to do a job they have been assigned or contracted to conduct, they are also considered to have a legitimate educational interest.
2. In order to allow Tynker to provide you with the Services, you hereby designate Tynker as a "school official" with a "legitimate educational interest" under FERPA in using and accessing your Education Records. You also represent and warrant to Tynker that (a) you have obtained all consents necessary in connection with disclosing any Education Records directly or indirectly to Tynker, or otherwise in connection with the Services, and (b) your disclosures described in (a) are not and will not be a violation of FERPA.
3. Educational Institutions may use the Services to automatically create accounts on behalf of its students, using Education Records to "pre-populate" those students' names and contact information into the accounts and providing Tynker with such information of the students. The student then chooses whether to activate an account with Tynker to enroll in online courses, take part in the class discussion, and use other features available through the Services. We treat that pre-populated content as the Educational Institution's confidential information; that means that we won't disclose it or use it, except as we're expressly required or allowed to under these Additional Terms, our Terms of Use and Privacy Policy. Once a student activates their account, any information in their account (even information pre-populated by Educational Institutions) belongs to them – we consider it disclosed by the individual (even if it was initially pre-populated by Educational Institutions). Therefore, post-activation, Tynker's use of content in a student's account is covered by Tynker's Privacy Policy.

III. Use of Data from Education Records

1. By disclosing or providing PII or other information from the Education Records to us, whether via the Services or otherwise, you expressly grant, and you represent and warrant that you have all rights necessary to grant, to us a non-exclusive, royalty-free, worldwide license to use, transmit, distribute, modify, reproduce, display, and store such information only for the purposes of providing the Services as contemplated in and enforcing our rights hereunder. Tynker will only use and access your Education Records as necessary to provide the Services to you, your students, instructors and professors, and only for authorized purposes in accordance with terms of these Additional Terms, Tynker's Terms of Use, and Privacy Policy. For clarity and without limitation, we will not (and will not allow third parties to) use PII from Education Records to engage in targeted advertising.
2. You agree that we may collect, share, publicly disclose, or otherwise use data derived from Education Records, including contextual or transactional data about a student's or a user's access and use of the Services, that has been anonymized, aggregated, or otherwise de-identified such that the data cannot reasonably identify a particular student, user, or an Educational Institution ("De-identified Metadata"). We may use any De-identified Metadata that is not linked to FERPA-protected information for other purposes, unless otherwise prohibited by the terms of these Additional Terms and Tynker's Terms of Use, such as to develop, evaluate, analyze, improve, operate, provide, or market our Services. You further agree that we may use, store, transmit, distribute, modify, copy, display, sublicense, and create derivative works of the De-identified Metadata even after this Agreement has expired or been terminated.

IV. Sharing of Data from Education Records

1. We treat the PII from Education Records as confidential and do not knowingly share it with third parties other than as described in Tynker's Terms of Use and Privacy Policy. We provide access to PII from Education Records only to our employees, contractors, and agents who have a need to access or use such information in connection with providing the Services to you and are subject to confidentiality obligations as strict as those under these Additional Terms. We will not sell, rent, share, or re-disclose PII from Education Records to other parties, unless we have specific authorization from you to do so and

it is otherwise permitted by FERPA. However, students may retain possession and control of their own student-generated content, if applicable, such as having the option to transfer such content to a personal account by sending us an email request at privacy AT tynker DOT com.

Project Creation

1. During the regular course of completing lessons, students create digital content ("Projects") and have access to Projects that are saved in their private account on Tynker. These are visible only to themselves and their teacher. Students can delete these Projects at any time.

Sharing Projects

1. Students and teachers can also share projects to Class Showcases that may be accessed by the teacher and a Limited User Group, such as their classmates. Teachers and administrators from the Educational Institution can remove these Projects from the Class Showcase. Although we do not allow students to post to social media sites, students may manually copy URL links to Tynker projects and post these links on other social media sites that may not allow deletion. In such cases, the student or educator can delete the original project and the links on external sites will no longer work.

Transferring Projects

1. Tynker Projects cannot be transferred to other accounts. However that can be copied over to other accounts. A new Project will be created in the other account and will be an exact replica of the original project. Deleting the original project will not delete the copy. The copy may be deleted at any time by the new owner of that copied Project.

V. Access and Deletion of Education Records

1. Tynker will use commercially reasonable efforts to comply with written requests from you or a Parent for access to and review their Education Records and to correct any erroneous information within a reasonable period of time, but not more than 45 days after we have received the request. You and Parents can submit such request by sending us an email request at privacy AT tynker DOT com. Whenever applicable, you will serve as

the intermediary for the requests by Parents, wherein the parent requests access to any Education Records created and maintained by Tynker directly from you, and you then obtain the Education Records from us to give back to the Parent.

2. Parents, legal guardians, or eligible pupils may review personally identifiable information in the pupil's records and correct erroneous information by the following protocol:
    - Removing or changing student Projects – Parents or kids can login to their child's account, and edit or delete Projects.
    - Changing PII (screen name, first name, last name, password, avatar) – Parents need to inform the class teacher.
    - Deleting the child's account – Parent can contact the School, and the teacher can perform this action. School may also contact Service Provider by sending an email to support AT tynker.com, and we will do so in 72 hours.
3. Educational Institutions and Parents may request Tynker in writing by sending an email to privacy AT tynker DOT com to terminate the Services and/or delete the PII from their Education Records maintained by Tynker. You understand that you and Parents may not be able to access or use certain portion of the Services after Tynker deleted the account and information pursuant to your or Parents' request. We will use commercially reasonable efforts to comply with such deletion request and we certify that we will not retain or otherwise make available to third parties the Education Records after the termination, except (i) as permitted hereunder, or (ii) if a student chooses to establish or maintain an account with Tynker for the purposes of storing student-generated content. However, we may de-identify student information [, including without limitation, by deleting or de-identifying all PII from Educational Records within seventy-two (72) hours of our receipt of the termination notice, except for Student Data residing on internal logs which will be removed within ninety (90) days, and will also provide notice to the Educational Institutions when PII from Educational Records has been deleted and/or anonymized] before we retain it, share it with other parties, or use it for other purposes.
4. Tynker may terminate these Additional Terms and Tynker's Terms of Use in accordance with the "Termination" section of Tynker's Terms of Use. All provisions of these Additional Terms and Tynker's Terms of Use, which, by their nature, should survive termination, shall survive termination, including,

without limitation, ownership provisions, warranty disclaimers, limitations of liability, indemnities, and governing law.

VI. Data Privacy, Confidentiality, and Security

1. Tynker maintains industry level administrative, physical, and technical measures to protect Education Records stored in our servers, which are located in the United States. We train our employees to ensure the security and confidentiality of Education Records maintained by us. If there is any unauthorized disclosure or access to any PII from Education Records, we will promptly notify you, any other affected Educational Institutions by email and will use reasonable efforts to cooperate with your or their investigations of the incident. We require that you inform the parents of all affected students, since Tynker may not have access to Parent contact information. As the owner of the Education Records, you may be responsible for the timing, content, cost, and method of any notice requirements trigged by security incidents under applicable laws. When permissible under applicable laws, you may request Tynker to bear responsibility for the timing, content and method of such required notice on your behalf. In all instances, Tynker will indemnify Educational Institutions for all reasonable costs associated with compliance with such notice requirements arising from a breach of the Services by Tynker. For clarity and without limitation, Tynker will not indemnify for any notification costs arising from a breach of you or a third party.

VII. Contact

1. Please refer to Tynker's Terms of Use and Privacy Policy for more details on use of Tynker's Services and our privacy practices. If you have any questions, complaints, or claims with respect to the Services, or anything in our Terms of Use, these Additional Terms, or our Privacy Policy, you may contact us at 650B Fremont Ave, #330, Los Altos, CA 94024 or privacy AT tynker DOT com. We'll do our best to promptly respond to you.

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" 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 [*check one*] _____will __x___will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, 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 MLSA," 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 MLSA 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 MLSA 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 MLSA.

(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 MLSA, 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 MLSA," 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)

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:

DocuSigned by:
Jean Blackwell
3C916E402F9E42D...
Signature

_**Jean Blackwell**_____
Printed Name

_Head of Education Partnerships _____
Title

5/5/2023
_____
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND [*NEURON FUEL, INC. DBA: TYNKER*]

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with [*Neuron Fuel, Inc. dba: Tynker*] which governs the availability to Participating Educational Agencies of the following Product(s):

[Tynker Junior K-2 Premium Curriculum
Tynker Elementary K-5 Premium Curriculum
Tynker Middle School 6-8 Premium Curriculum
Tynker K-8 Premium Curriculum
Tynker High School 9-12 Premium Curriculum
AP Computer Science A
AP Computer Science Principles
]

Pursuant to the MLSA, 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 MLSA. 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 MLSA (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 MLSA 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: [NA]

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA 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 Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master 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.