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, but that adoption may not occur until a date subsequent to the effective date of the MLSA. Erie 1 BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption., 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 MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA:

Graide Network Data Security and Privacy Plan

As our first and top priority prior to launching, The Graide Network engaged Franczek Radelet, a premier education firm, to assist with understanding and assessing student records and privacy issues associated with our company. We wanted to ensure that our practices complied with all student privacy and student data laws and guidelines and met all federal legal protections for personally identifiable student records.

Compliance with these privacy laws primarily is the responsibility of school districts, schools, and school employees. Similarly, the penalties for non-compliance primarily fall on the same. At The Graide Network, however, we take our commitment to student privacy very seriously. We strive to be a trusted school partner, and as such, we are committed to complying with the relevant laws even when they do not directly relegate The Graide Network.

FERPA Overview

The primary law that governs student records privacy is the federal Family Educational and Privacy Rights Act ("FERPA"). FERPA gives parents/guardians and students a number of rights and protections, the most applicable of which is a general requirement of confidentiality for any student identifying records or information. Under the law, schools are generally prohibited from sharing student identifying records or information with third parties without express, written parental/guardian consent or, in the case of a student who has reached 18 years of age (called an "eligible student" under FERPA and in this memorandum), student consent.

Under FERPA, for instance, schools are generally prohibited from sharing "education records" and "personally identifiable information" ("PII") with any individual, agency, or organization without the written consent of the parent/guardian or eligible student. 20 U.S.C. §1232g(b)(1). FERPA defines "education records" as "those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution." 20 U.S.C. §1232g(a)(4)(A). Regulations implementing FERPA provide a list of things that can be "PII," including, most importantly for The Graide Network, a broad catchall including "information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty." 94 CFR § 99.3.

There is little question that unredacted student work that includes student names, student markings, and other potentially identifying information and that has been collected by a teacher and provided to a Graide Network TA for analysis and grading would fall under the definitions of "education records," "PII," and "student records" under FERPA. There may be exceptions where certain student work does not fall within these definitions, but we take a conservative approach to compliance with the law and consider all original work collected by teachers and provided to Graide Network TAs as within the scope of protected information under FERPA.

School Official Exception

FERPA has numerous exceptions that allow for disclosure of protected student identifying information without consent, including the "school official" exception. Under FERPA, disclosure may be made without parental/guardian or eligible student consent to "other school officials, including teachers within the educational institution or local educational agency, who have been determined by such agency or institution to have legitimate educational interests, including the educational interests of the child for whom consent would otherwise be required." 20 U.S.C. §1232g(b)(1)(A). The FERPA regulations further define "school officials" to include "[a] contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions." 34 C.F.R. § 99.31(a)(1)(i)(B).

Notably, FERPA's school official exception only allows disclosure of PII to a third party service provider like The Graide Network without parental or eligible student consent if all of the following conditions are met:

1. The provider performs an institutional service or function for which the school district would otherwise use its own employees;
2. 2. The provider has been determined to meet the criteria set forth in the school district's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records;
3. 3. The provider is under the direct control of the school district with regard to the use and maintenance of education records, which includes that the school district controls and dictates how the provider can use or cannot use the data that is shared; and
4. The provider uses education records only for authorized purposes and may not re-disclose PII from education records to other parties (unless the provider has specific authorization from the school district to do so and it is otherwise permitted by FERPA).

With respect to the first requirement, The Graide Network TAs perform an institutional service or function (namely, grading and feedback) for which the school district would otherwise use its own employees. The U.S. Department of Education advises school districts subject to FERPA that they are not precluded from disclosing education records to parties to whom they have outsourced services so long as they do so under the same conditions applicable to school officials who are actually employed. See U.S. Dep't of Educ. Letter to Clark County Sch. Dist. NV re: Disclosure of Education Records to Outside Service Providers (June 28, 2006). Here, the work conducted by Graide Network TAs is work otherwise conducted by teachers, aides, student teachers, or TAs employed by the school, and the work of Graide Network employees in supervising that TA work is work that would otherwise be conducted by teachers or administrators. Numerous educational technology organizations with an even more attenuated relationship to the classroom than The Graide Network regularly rely on the school official exemption. For example, Google Apps for Education relies on the exemption to provide email and other productivity tools for schools that are much farther removed from the traditional services provided by school districts than The Graide Network's work.

With respect to the second requirement, the notification of FERPA rights is something that

schools must publish each year (usually in a handbook) to notify parents/guardians/students of what types of entities can be deemed school officials. The Graide Network requires evidence of compliance with this requirement from teachers or school administrators before allowing them to submit student identifying information.

With respect to the third and fourth requirements, The Graide Network meets these obligations through a) contracting with the school district through individual teachers or principals, with the understanding that they will have obtained appropriate authority from their school districts, or b) contracting directly with the school district through an authorized administrator.

Our Three-Pronged Approach to Student Privacy

We appreciate the sensitivity of student data issues for schools, parents/guardians, and students. Federal and state laws require confidentiality for any student identifying records or information. This data includes any and all Personally Identifiable Information (PII) and other non-public information that a teacher shares on The Graide Network ("Data"). Data include, but are not limited to, student data, metadata, and user content.

Our three-pronged approach to ensuring compliance with student records privacy is as follows:

First, Graiders are required to sign a confidentiality agreement that they may not re-disclose information shared with them with any third party or use the information shared for any purpose other than the agreed-upon work with the teacher who provided the information. Graiders do NOT work directly with students. As aspiring teachers, Graiders are receiving similar education on the importance of student privacy from their teacher preparation program, including even more rigorous requirements for student teaching placements. They take their legal responsibilities seriously as compliance directly relates to their professional goals.

Second, we require teachers to obtain the proper approvals from an authorized school administrator before working with a Graider. Teachers must adhere to one of the following prior to uploading any student work to the Site:

1. Have an authorized administrator from your school enter into an agreement directly with The Graide Network (the best option—more on that later); or
2. Obtain permission from a school administrator with authority to enter into contracts on behalf of the school district; or
3. Obtain parent permission to share the student identifying information; or
4. Redact all student identifying information (e.g., assign each student a number and have them write it on their assignment instead of their name)

For the third option, the written consent must contain all of the following:

- Signature of the parent/guardian or eligible student;
- The date of the written consent;
- Specification of the records to be disclosed;
- A statement of the purpose of the disclosure; and
- Identification of the party or class of parties to whom the disclosure may be made.

The consent may be obtained electronically, but only if it is obtained in a way that: (1) identifies and authenticates the particular person as the source of the consent; and (2) indicates such person's approval of the information contained in the consent. Further, if information is shared by a Teacher through a "shared drive," access may only be given to information for which there is adequate consent.

Third, we as a company collect as little data as possible about students and will not use that data to advertise or market to students or their parents. Student-identifying records or information on Site may be shared with administrators and other school employees pursuant to the school district's policies and procedures. The Graide Network will not use any Data to advertise or market to students or their parents. Advertising or marketing may be directed to schools or districts only if student information is properly de-identified.

How We Use Data

Student-identifying records or information on the Site may be shared with The Graide Network employees for quality control measures. We will use Data only for the purpose of fulfilling our duties and providing services under our agreements with schools and for improving services. The Graide Network may use de-identified Data for product development, research, or other purposes.

De-identified Data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, location information, and school ID. Furthermore, The Graide Network agrees not to attempt to re-identify de-identified Data and not to transfer de-identified Data to any party unless that party agrees not to attempt re-identification.

School partners understand that we will rely on one or more subcontractors to perform our services. We agree to share the names of these subcontractors with school partners upon request. All subcontractors and successor entities of The Graide Network will be subject to the terms of this Privacy Pledge.

Data Security

We store and process Data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. We will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

The Graide Network has a written incident response plan, to include prompt notification of school partners in the event of a security or privacy incident, as well as best practices for responding to a breach of PII. We will notify teachers and school partners immediately upon any material changes to this privacy policy.

(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*] ___X___will _____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 subcontactors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontactors, 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)

ERIE 1 BOCES

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

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:

Signature

Elizabeth Nell

Printed Name

Co-Founder and Head of Sales

Title

05 / 22 / 2020

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND [*THE GRAIDE NETWORK, INC.*]

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

[*Classroom Writing and Writing Benchmarks*]

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: [*Before commencing work with The Graide Network, every Graide must sign a legally binding non-disclosure agreement including acknowledgment of their obligation under Section 2-d of the New York State Education.*]

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on [May 22, 2020] and expires on [June 30, 2023 at 11:50 pm].
- 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.