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.

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:

The Social Express ("**LEX,**" "**we**" or "**us**") provides educational materials and related services, via a set of online learning platforms. The following privacy policy governs our privacy practices for each learning platform that links to this policy.

- **Our Commitment to Privacy**

We have created our learning platform to assist schools in providing personalized and rewarding online educational experiences to their students. We believe that transparent and strong privacy practices foster these experiences, and we provide this privacy policy in that spirit.

- **Our Compliance With COPPA And FERPA**

Our learning platform is designed for schools and teachers working with K–12 students. We recognize the sensitive nature of personal information concerning students under age 13, and concerning K–12 students generally, where the information is contained in a school's educational records. This personal information is protected under either or both of the following federal statutes: the Children's Online Privacy Protection Act ("COPPA") and the Family Educational Rights and Privacy Act, including the Protection of Pupil Rights Amendment ("FERPA"). Our privacy practices comply with both COPPA and FERPA.

- **The Scope of Our Privacy Policy**

This privacy policy governs our privacy practices with respect to all personal information that our users submit, or that we collect in connection with our learning platform. This policy governs not only our practices with respect to students' personal information, but also with respect to the personal information of teachers and school administrators who use our learning platform.

- **Consent from Schools regarding Students' Personal Information**

COPPA permits a school, acting in the role of "parent," to provide required consents regarding personal information of students who are under the age of 13. Where a school is the subscriber to our learning platform, we rely on this form of COPPA consent. We provide the school with this privacy policy, to ensure that the school, in providing its COPPA consent, has full information and assurance that our practices comply with COPPA.

FERPA permits a school to provide educational records (including those that contain students' personal information) to certain service providers without requiring the school to obtain specific parental consent. FERPA permits this where the service provider acts as a type of "school

official" by performing services, for example, that would otherwise be performed by the school's own employees. We fulfill FERPA requirements for qualifying as a school official by, among other steps, giving the school direct control with respect to the use and maintenance of the education records at issue (including associated personal information), and refraining from re-disclosing or using this personal information except for purposes of providing our learning platform to the school. We comply with FERPA by relying on this form of consent.

- **Consents from Other Users**

We also obtain consents regarding personal information of users other than students (such as teachers and school administrators). To obtain these consents we (a) notify the users of our privacy practices by including links to this privacy policy within our learning platform, and (b) rely on their continued use of our learning platform to indicate their consent to this privacy policy.

- **The Types of User Information We Collect**

We limit our collection of personal information to no more than is reasonably necessary for the user at issue to participate in our learning platform. Specifically, we collect the following types of information:

- **School Administrator Information: we collect registration information from a school administrator when the school administrator activates the school's subscription account, which may include the school administrator's own first and last name, business address and phone number, date of birth, email address, and username;**
- **Teacher Information: we collect registration information from a teacher or school administrator when the teacher (or school administrator) activates the teacher's account, which may include the teacher's first and last name, email address, and username and assessments.**
- **Student Information: we collect registration information from a teacher or school administrator when the teacher (or school administrator) activates the account of an individual student, which may include the student's first and last name, grade level for reading comprehension, email address and username.**
- **Schoolwork Information: we collect information contained in student assessments/quizzes/surveys.**
- **Usage Information: we collect usage, viewing & analytics.**

If we discover that we have collected information in a manner inconsistent with the requirements of COPPA or FERPA, we will either (a) delete the information or (b) promptly seek requisite consents before taking further action concerning the information.

- **How We Collect Personal Information**

Our learning platform collects personal information in two ways. First, school administrators and teachers provide personal information during the registration process. Second, teachers have access to student quiz scores and assessments/surveys.we collect usage information through technology, such as cookies, flash cookies, web beacons, and persistent identifiers. This collection of usage information takes place, for example, when a student or other user visits our learning platform, and during the activities in which the user engages. Certain features (or all features) of our learning platform may be hosted on third party sites, and in those instances the collection activities described above are undertaken by this third party, under our direction and control and consistent with this privacy policy.

- **How We Use Personal Information**

We use personal information for the following purposes:

- **To provide users with the content and features available through our learning platform;**
- **To communicate with school administrators and teachers about the applicable subscription account or transactions with us, and to send information about our learning platform's features and, where applicable, changes to these features;**
- **To personalize our learning platform's content and experiences for students, teachers, and other users of the platform; and**
- **To detect, investigate and prevent activities that may violate our policies or be illegal.**

We do not as a rule allow third-party operators to collect personal information or usage information through persistent identifiers on our learning platform for any purposes other than the internal operations of our platform. Further, we do not use personal information collected through our Platform for the purpose of targeted advertising.

Finally, we de-identify usage information in accordance with COPPA and FERPA, and use this de-identified information to develop, evaluate, and provide improved educational products and services, as permitted under COPPA and FERPA. To the extent we collect information that constitutes Performance Review Data, we protect such information as personal information in accordance with this Privacy Policy.

- **We Do Not Share Personal Information Beyond Our Learning Platform Except In Specific, Limited Circumstances**

We use personal information for our internal purposes only, with the following limited exceptions. First, we share information with our service providers if necessary for them to perform a business, professional, or technology support function for us. In instances where we engage service providers for these purposes, we require them to comply with this privacy policy. Second, we disclose personal information:

- **In response to the request of a law enforcement agency or other authorized public agency, including a request by a children's services agency or by the school at issue;**
- **To protect the security or integrity of our learning platform and associated applications and technology, as well as the technology of our service providers;**
- **To enable us to take precautions against liability, enforce legal rights, and to detect, investigate and prevent activities that violate our policies or that are illegal;**
- **If we are directed to do so by a subscribing school in connection with an investigation related to public safety, the safety of a student, or the violation of a school policy; and**
- **In other cases if we believe in good faith that disclosure is required by law.**

- **How We Protect Personal Information**

We have implemented and maintain technical, administrative and physical security controls that are designed to protect the security, confidentiality and integrity of personal information collected through our learning platform from unauthorized access, disclosure, use or modification. Our information security controls comply with reasonable and accepted industry practice, as well as requirements under COPPA and FERPA. We diligently follow these information security controls and periodically review and test our information security controls to keep them current.

- **1 Information Security Procedures**. We will:
  - **Standard of Care. Keep and maintain all personal information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, modification, or disclosure;**
  - **Use for School Purposes Only. Collect, use, and disclose personal information solely and exclusively for the purposes for which you provided the personal information, or access to it to us, and not use, sell, rent, transfer, distribute, modify, data mine, or otherwise disclose or make available personal information for our own purposes or for the benefit of anyone other than the school, without the school's prior written consent;**
  - **Non-Disclosure. Not, directly or indirectly, disclose personal information to any person other than our employees and service providers who have a need to know, without express written consent from the school;**
  - **No Commingling. Segregate (via logical, database, or physical segregation) personal information from our other information or our other customers so that a school's users' personal information is not commingled with any other types of information not related to the school;**
  - **Employee Training. Provide appropriate privacy and information security training to our employees.**
  - **Transport Security. Use Transport Layer Security (TLS) for the transmission of all user data to and from our learning platform; and**
  - **Secure Storage. Use industry standard file encryption for user data that is subject to protection under either COPPA, FERPA, or both. Where file**

encryption is not reasonably feasible, we employ other industry standard safeguards, protections, and countermeasures to protect such data, including authentication and access controls within media, applications, operating systems and equipment.

- **2 Data Location and Security.**We use cloud service providers in the delivery and operation of our learning platform(s), and data (including personal information) is stored on the servers of our cloud service providers. Our contracts with our cloud service providers requires them to implement reasonable and appropriate measures designed to secure content against accidental or unlawful loss, access, or disclosure. Our cloud service providers have at least the following security measures in place for their networks and systems: (i) secure HTTP access (HTTPS) points for customer access, (ii) built-in firewalls, (iii) tested incident response program, (iv) resilient infrastructure and computing environments, (v) ITIL based patch management system, (vi) high physical security based on SSAE-16 standards, and (vii) documented change control processes. To the extent we store personal information internally on our servers, we comply with the information security controls set out in Section 10.1.
- **3 Data Breach Response.**In the event of a security breach involving Personal Information, we will take prompt steps to mitigate the breach, evaluate and respond to the intrusion, and cooperate and assist schools and other subscribers in efforts with respect to (i) responding to the breach, including the provision of notices to data subjects; and (ii) engaging mutually agreeable auditors or examiners in connection with the security breach, subject to reasonable notice, access and confidentiality limitations.

- **Access and Control of Personal Information**

School administrators and (where applicable) teachers hold access to personal information of the students for whom they are responsible, and they are able to update this information in the manner permitted by our learning platform. School administrators and teachers are similarly able to access and update their own personal information. The parents of a student can obtain access — through their child's school — to information concerning their child that is available on our learning platform. To do so, the parent should follow the school's procedures for access under FERPA. We cooperate with and facilitate the school's response to these access requests. Where the school's procedures do not apply to the parent's access request (and the request is otherwise proper), we will ourselves fulfill the request if and as required by law. After fulfilling an access request, we will update and (where necessary) correct the personal information at issue, as requested by the school or individual entitled to such access. We limit access to personal information to only those employees (i) who have a need to know such information, and (ii) who use the information only for the educational purposes of operating our learning platform and delivering our services.

- **Our Retention and Deletion of Personal Information**

We retain personal information of users of our learning platform (i) for so long as reasonably necessary (ii) to permit the user to participate in the platform, (iii) to ensure the security of our

users and our services, or (iv) as required by law or contractual commitment. After this period has expired, we will delete the personal information from our systems. Please understand that these deletion periods apply to personal information and do not apply to de-identified information. We retain de-identified information in accordance with our standard practices for similar information, and do not retain or delete such information in accordance with this policy.

In addition, if requested by a school, we will delete from our platform the personal information of the school's users, including its teachers and students, as the school directs. Deleting this information will prevent the school user from engaging in some or all features of our learning platform. Where required by local law, we will delete such information and provide a certification of such deletion.

- **NY Parents' Bill of Rights for Data Privacy and Security**

The New York Parents' Bill of Rights for Data Privacy and Security (the "**Privacy Bill of Rights**") addresses the relationship between schools and their third party contractors in addition to the schools' relationships with parents. The only elements of the Privacy Bill of Rights that are incorporated herein are those provisions directed to third party contractors ("**Contractor Privacy Provisions**"). LEX agrees to comply with the Contractor Privacy Provisions for schools in the State of New York. In the event of a direct conflict between this Privacy Policy and the Privacy Bill of Rights, the Privacy Bill of Rights will control. The full text of the Privacy Bill of Rights is available at http://www.p12.nysed.gov/docs/parents-bill-of-rights.pdf.

- **Definitions**

"De-identified information" means information that meets each of the following criteria: the information (i) does not identify a particular natural person; (ii) does not identify, by network Internet Protocol address, raw hardware serial number, or raw MAC address, a particular device or computer associated with or used by a person; (iii) does not identify the school at issue by name or address; and (iv) is not reasonably linkable to a particular natural person or school because of technical, legal, or other controls.

"Learning platform" means any LEX learning platform that links to this privacy policy.

"Parent" means a parent or legal guardian of a student.

"Personal Information" means information that identifies a natural person, as specified in the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, including the Protection of Pupil Rights Amendment ("FERPA") and the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 ("COPPA"), the California Student Online Personal Information Protection Act, Ch. 22.2, §§ 22584 et seq. of the California Business and Professions Code, and Section 49073.1 of the California Education Code.

"Student" means an individual receiving educational instruction via our learning platform. The term "student" includes individuals within the K–12 age group, and individuals who are children under the age of 13.

"Usage Information" means information that does not directly identify a particular person, but that may be linkable to a particular computer or device (via a unique device ID or otherwise).

"We" or "us" or "our" refers to LEX.

- **Contact Us**

You may contact us with questions or concerns with respect to this Privacy Policy at the following addresses: contact@socialexpress.com Any improper collection or misuse of information provided by LEX's Website is a violation of the Terms of Use and should be reported to contact@socialexpress.com If you have any questions about this Privacy Policy, please contact us at contact@socialexpress.com or write us at:

The Social Express
162 South Rancho Santa Fe Drive.
Suite E 70
Box 208
Encinitas, CA 92024

You may also telephone us at (877) 360.0155. (If you are not 18 years of age or older, you must have your parent or guardian's permission to call this number.)
Please be assured that any personal information that you provide in communications to the above e-mail and postal mail addresses and telephone numbers will not be used to send you promotional materials, unless you so request.

- **Effective Date**

The effective date of this Privacy Policy is July 7th, 2017.

(b) Insert here – also provide a copy of Data Security and Privacy Plan]

(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 _____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 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 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: The Language Express, Inc.

DocuSigned by:
Marc Zimmerman
E3DD911F1128401...
Signature

Marc Zimmerman
Printed Name

CEO
Title

5/3/2023
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND [THE LANGUAGE EXPRESS, INC.]

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

The Social Express

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 subcontactors, 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 subcontactors, 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 subcontactors, assignees, or other authorized agents abide by the provisions of these agreements by: [*Describe steps the Vendor will take*]

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1st, 2023 and expires on June 30th, 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.