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: https://learnplatform.com/data-processing-agreement

Data Processing Agreement

LearnPlatform, Inc., a North Carolina corporation with an address at 517 W. North Street, Raleigh, NC 27603 ("Provider") hereby agrees to the terms of this Data Confidentiality and Security Agreement ("Security Agreement") for the purpose of receiving and sharing confidential student information between a Local Education Agency ("LEA") in a manner consistent with the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and its implementing regulations at 34 CFR part 99; the Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. 1232h and its implementing regulations at 34 CFR part 98; the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501- 6506 and its implementing regulations at 16 CFR part 312; N.C. Gen. Stat. §§ 115C-401.1 and 115C-402; and the LEA's applicable regulations and procedures; and other applicable laws and policies.

1. **Purpose**. LEA is a local education agency that maintains student "education records" as defined by FERPA and PPRA. Provider is requesting access to certain student data maintained by LEA for the purpose of evaluating and/or providing educational products to LEA pursuant to a Subscription and License Agreement entered into concurrently herewith. The purpose of this Security Agreement is to set forth the terms and conditions upon which Provider may be granted access to such student data in order to ensure that the student data is used and stored appropriately and in compliance with all applicable federal, state, and local laws, regulations, and policies.

2. **Student Records and Information**. Provider acknowledges that any data shared and released to Provider by LEA (the "Shared Data") is for the sole purpose of evaluating educational products and services to enhance, supplement, and improve instruction for students. The Shared Data is defined as any data or information shared with Provider pursuant to this Agreement, including but not limited to any de-identified data, aggregated data sets, personally identifiable information (PII) about students, and other student information, including, but not limited to, student data, metadata, and user content. The Shared Data will be used by Provider for the sole purpose of evaluating educational products to inform instructional, operational and fiscal decisions, and the practices and processes related to education technology in schools, and for improving services under this Agreement. The parties agree that the Shared Data and all rights to the Shared Data, shall remain the exclusive property of LEA; provided however, that the analysis of the Shared Data performed by the Provider ("Results"), including without limitation the de-identified aggregate of the Shared Data, shall as between LEA and the Provider be the exclusive property of Provider. For the avoidance of doubt, de-identified aggregate data will have all direct and indirect personal identifiers removed, including, but not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. Provider agrees not to attempt to re-identify any deidentified data. Provider hereby grants to LEA a limited, nonexclusive, license to use the Results solely for its internal planning and purchasing decisions. LEA hereby grants to Provider a limited, nonexclusive, irrevocable license to use the Shared Data for the purpose of evaluating educational products and services as set forth in this Agreement.

3. **Compliance with Applicable Laws, Policies, and Procedures**. To become or remain a recipient of the Shared Data, Provider agrees to comply with the provisions of FERPA, PPRA, COPPA, and all other applicable laws and regulations in all respects. Nothing in

this Security Agreement may be construed to allow Provider to maintain, use, or disclose any Shared Data in a manner inconsistent with any applicable law, regulation, or policy.

4. **Authorized Use of Shared Data**. In the event Provider's access to the Shared Data is pursuant the "school official exception" as set forth in 34 CFR 99.31(a)(1)(i), Provider's use of the Shared Data shall at all times be limited to institutional functions of LEA that could otherwise be provided by a school official and which LEA is "outsourcing" to Provider pursuant to 34 CFR 99.31(a)(1)(B). Provider agrees to use the Shared Data for no other purpose other than those identified in Paragraph 2 of this Agreement. Provider understands that the Security Agreement does not convey ownership of Shared Data to Provider. Provider specifically acknowledges that Provider's use of the Shared Data and Results in connection with any marketing activities shall not exceed the acceptable uses permitted by 20 U.S.C. § 1232h(c)(4)(A).

5. **Procedures for the Maintenance and Security of Shared Data**. While in the possession, custody, or control of Provider, all Shared Data shall be stored in a secure environment with access limited to the least number of staff needed to complete the work requested by LEA. Provider shall develop, implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentiality, integrity, and availability of all electronically maintained or transmitted data received from, or on behalf of, LEA. Such measures shall include processes for transmission and storage of such data.

a. Provider agrees that it will protect the Shared Data against loss, destruction, and unauthorized uses or disclosures according to industry best practices and no less rigorously than it protects its own confidential information. Specifically, Provider agrees that all student records and PII obtained in the course of providing services to LEA shall be subject to the confidentiality and disclosure provisions of applicable federal and state statutes and regulations.

b. For the purposes of ensuring Provider's compliance with this Security Agreement and all applicable state and federal laws, Provider shall designate one or more individuals as the primary data custodian(s) of the data that the LEA shares with Provider and shall notify LEA of the name(s) and title(s) of such individual(s) prior to any data being shared. LEA will release all data and information for this project to the named primary data custodian(s). The primary data custodian(s) shall ensure that the project shall be conducted in a manner that does not permit personal identification of the LEA's students by anyone other than representatives of Provider who need such information for the purposes described in Paragraphs 1 and 2 of this Security Agreement. The primary data custodian(s) shall also be responsible for maintaining a log of all data received pursuant to this Security Agreement and ensuring the timely destruction or return of the Shared Data as required by this Security Agreement.

c. Provider shall use industry best practices to protect LEA's data from unauthorized physical and electronic access no less rigorously than it protects its own confidential information. All LEA data shall be kept in a secure location preventing access by unauthorized individuals. Provider shall not forward to any person or entity other than LEA any student record or PII, including, but not limited to, the student's identity, without the advance written consent of LEA. Provider agrees to handle any and all Shared Data using appropriate access control and security, including password-protection and encryption in transport and electronic storage, and periodic auditing of data at rest. Data subject to FERPA shall not be emailed in plain text or used for marketing campaigns. Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

d. Provider will maintain an access log delineating the date, time, and identity of any person or entity given access to any Shared Data student records who is not in the direct employ of Provider. No such access shall be granted except in strict compliance with the terms and conditions of this Agreement and applicable law.

6. **Prohibition on Unauthorized Use or Disclosure of Shared Data.**

a. Provider agrees to hold all Shared Data in strict confidence. Provider shall not use or disclose such data received from or on behalf of LEA except as authorized in this Agreement or otherwise in writing by LEA or as required by law. Provider agrees not to disclose any data obtained from LEA in a manner that could identify any individual student to any other entity or person, attempt to infer or deduce the identity of any individual student based on data provided by LEA, or claim to have identified or deduced the identity of any student based on data provided by LEA.

b. Provider is prohibited from mining Shared Data for any purposes other than those set forth in this Agreement or otherwise agreed to in advance writing by LEA. Data mining or scanning of user content for the purpose of advertising and/or marketing any non-educational products or services to students or their parents is strictly prohibited.

c. In no event will Provider use any of the Shared Data for its own commercial marketing or advertising purposes, or for the commercial marketing or advertising purposes of any third-party. Without limiting the foregoing, LEA and Provider agree that use of the Results for Provider's marketing or advertising purposes is permitted so long as no individual student's identity is disclosed or capable of being deduced. Provider will not use any Shared Data to advertise or market non-educational products or services to LEA students or their parents.

d. In the event of any unauthorized use or disclosure, Provider shall report the incident to LEA no less than one (1) business day after Provider learns of such use or disclosure. Such report shall identify:

i. The nature of the unauthorized use or disclosure,

ii. The data used or disclosed,

iii. Who made the unauthorized use or received the unauthorized disclosure,

iv. What Provider has done or shall do to mitigate the effects of the unauthorized use or disclosure, and

v. What corrective action Provider has taken or shall take to prevent future similar unauthorized use or disclosure. Provider shall also provide such other information related to the unauthorized use or disclosure that may be reasonably requested by LEA. LEA also may require that Provider provide a written notice of the breach or disclosure, as well as a description of the corrective actions taken, to any LEA student, parent, or employee directly impacted by the breach or disclosure. Any such notice shall be subject to review and approval by LEA.

e. Provider will not release any research or publications pertaining to LEA's data and through which LEA is named or can be identified without LEA's advance written consent.

7. **Employees, Contractors, and Agents.** Provider may only share the Shared Data, or any part of it, with subcontractors who have agreed in writing to adhere to, and be bound by, all of the terms of this Security Agreement with respect to its possession and use of any Shared Data and acknowledging that the subcontractor is aware of its obligations under applicable law with regard to the possession, use and re-disclosure of the Shared Data. LEA reserves the right to request to review and approve any such agreement between Provider and its subcontractor(s) before any Shared Data is disclosed to the subcontractor(s). Nothing in this paragraph shall relieve Provider of any its obligations under this Agreement, including its responsibilities to ensure the security of any Shared Data provided by LEA pursuant to this Agreement.

8. **Monitoring and Auditing.** Any Shared Data held by Provider will be made available to LEA for review and inspection upon request of LEA. Provider shall cooperate with LEA or with any other person or agency as directed by LEA, in monitoring, auditing, or investigating activities related to Provider's use and safeguarding of the Shared Data, including but not limited to allowing inspection of the data logs described in Paragraph 5.b and 5.d of this Agreement. LEA and its auditors will maintain the confidentiality of any confidential information and trade secrets of Provider that may be accessed during an audit conducted under this Security Agreement.

9. **Term; Post-Termination.** This Security Agreement takes effect upon the date of full execution and continues in full force and effect for so long as Recipient has possession, custody, or control of any of the Shared Data. Upon the termination of this Security Agreement between LEA and Provider, all Shared Data shall, at LEA' sole option, be destroyed or returned to LEA. No other entity, including any subcontractors of Provider, shall be authorized to continue possessing or using any Shared Data. Any Shared Data remaining on any computers, servers, or other technological devices of Provider or its employees, agents, or subcontractors, shall be permanently deleted.

10. **Breach and Default; Indemnification; Remedies.**

a. In the event of a material data or security breach, or, breach of any other material term of this Security Agreement, LEA may demand the immediate return or destruction of any and all of the Shared Data.

b. Provider shall fully indemnify and hold harmless the LEA's Board of Education and its past, current and future members, agents, and employees from and against all claims, actions, demands, costs, damages, losses, and/or expenses of any kind whatsoever proximately resulting from any material data breach of this Security Agreement or any unauthorized use or disclosure of the Shared Data by Provider or it's subcontractor(s). This section shall survive the expiration or earlier termination of this Security Agreement.

c. Nothing in this Agreement shall restrict LEA from seeking any other rights or remedies to which it may be entitled at law or equity.

11. **No Right or Entitlement to Student Data.** This Security Agreement sets out the terms and conditions, under which LEA may, in its sole discretion, provide Shared Data to Provider. Nothing in this Security Agreement creates any right, title, or interest in Recipient to receive any such information.

12. **Miscellaneous.**

a. Governing Law. This Security Agreement and the rights and obligations of the parties hereto shall be governed by and construed and enforced in accordance with the laws of the State of North Carolina.

b. No Third Party Beneficiaries. Nothing in this Security Agreement shall confer upon any person, other than the parties, any rights, remedies, obligations, or liabilities whatsoever.

c. Counterparts. This Security Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

d. Headings. The headings and other captions in this Security Agreement are for convenience and reference only and shall not be used in interpreting, construing or enforcing any of the provisions of this Security Agreement.

e. Assignment of Rights. Neither this Security Agreement, nor any rights, duties, nor obligations described herein shall be assigned by Provider without the prior express written consent of LEA. Notwithstanding the foregoing, Provider may assign all of its rights under this Agreement, without consent of LEA, to a successor by merger or acquisition or to any person or entity who purchases all or substantially all of the business or assets of Provider to which this Agreement relates.

f. Entire Agreement; Amendment. This Agreement contains the entire agreement between the parties and supersedes any previous agreements and proposals, oral or written, related to the subject matter hereof. Any modification or amendments to this Agreement shall be effective only if made in writing and signed by both parties.

g. Conflicts. In the event of any conflict between this Security Agreement and any existing or future contract, purchase order, agreement or terms of service between LEA and Provider, the terms and conditions of this Security Agreement shall control.

(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. <u>Additional Statutory and Regulatory Obligations</u>

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:

Matt Doherty

Signature

Matthew Doherty

Printed Name

Chief Operating Officer

Title

May 29, 2020

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND LEARNPLATFORM

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with LearnPlatform which governs the availability to Participating Educational Agencies of the following Product(s):

LearnPlatform subscriptions

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: Sub-Contractors sign the LearnPlatform Business Protection Agreement that reflects terms in compliance with the MLSA. For those organizations for which LearnPlatform relies to provide hosting services, the data security agreements provide for SLA and data privacy agreements.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on May 4, 2020 and expires on June 30, 2023.
- 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.