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 Services 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) "**Participating Educational Agency**" means a school district within New York State that has the right to access and use 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.

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

(c) "**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.

(d) "**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.

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:

Mesa Cloud Data & Privacy Plan

Cloud Policy and Physical Safeguards.

- Provide training to all personnel on federal and state law governing confidentiality to ensure proper safeguard measures to ensure security, confidentiality and integrity of personally identifiable information ("**PII**").
- Limit internal access to PII only to those individuals that are determined to have a legitimate need for accessing educational data in accordance with the Principle of Least Privilege.
- Maintains reasonable administrative, technical, physical safeguards to protect the security, confidentiality, and integrity of education records in its custody including (a) securing suite in office building only accessible by lock/key and additional remote buzzer for entry, (b) ensuring that all computers/desktops are password protected and only accessible by authorized personnel and (c) storing all physical documents in locked file cabinets.
- All PII is stored on AWS, our host provider. Vendor hosts a FTP Server with Files.com that also contains district-provided data (i.e., PII). Vendor collects what NIST classifies as less-used personal identification, including Full Name, State, Country, Gender/Race. Vendor does NOT collect the following:
    - National ID numbers (SSN, etc.)
    - Bank account numbers
    - Passport numbers
    - Drivers License numbers
    - Credit Card numbers

Encryption.

Vendor will encrypt data in motion or in custody from unauthorized disclosure, using technology or methodology specified by the secretary of the US Department of Health and Human Services in guidance issued under Sec 13402 (h)(2) of Public Law 111-5. Encryption at rest.

File encryption, Database security, secured algorithms, controlled port access assures data at rest. Data is formatted in raw format during execution and access creating cipher code regeneration. Data at Rest is a stationary data, post data execution, data is migrated to storage devices following IPsec cipher with use of integral database engines.

Encryption in Motion.
Clear text data captured via portal will be over SSL layer along with last mile 128 bit SSL sealed encryption monitored and provided by industry leader solution providers. Post motion data at rest procedures. Vendor uses a minimum 4096-bit RSA keys.

Breach Plan and Notification.

Vendor will notify BOCES upon any breach of security resulting in an unauthorized release of student data by Vendor or its assignees in violation of State or Federal law or regulation, Parents Bill of Rights for student data privacy and security, the data privacy and security policies and procedures of BOCES and/or building contractual obligations relations to data privacy insecurity. Notification will be sent in the most expedient way practicable and without unreasonable delay.

Technical Protocol.

• Vendor on-Time, along with internal infrastructure are protected with managed and automated monitoring services and threat countermeasures. Both Vendor's WAN and internal services are continuously monitored for threats. An electronics notification system will self-alert our administrative team about possible breach or potential attack. Security governance process will identify the level of breach and if a breach occurred. It will address via defined code of processor and countermeasures. Breach will be immediately reported to required authorities, along with severity, cause of damage, possibility of damage, and action plan along with deadlines for the remedy.
• Other measures to further prevent and monitor threats will be provided via third-party providers and partners.

Data Disclosure.

Vendor will not disclose provided data other than to its employees who need to work with such provided data under this Agreement. Vendor will not use provided data for any other purposes than those explicitly provided for in this Agreement. All provided data shall remain the property of the disclosing party. Personally identifiable information or data that is provided to the Provider will not be sold or used for marketing purposes.

Data Return.

• Data will be returned to BOCES and/or destroyed upon termination/expiration of the Agreement or as directed by BOCES.
• A report will be submitted to official for approval to purge. Affirmation for purging data is required within 7 days of the reported date. Transition data will be offloaded from production environment. Once purged sequence initiated, data will be permanently destroyed, beyond the point of recovery. Prior to purge action, Official may request a copy of the data for their safekeeping, solely at their will and at their custody and encryption protected. Encryption key will need to be provided by official and we will not have any access or control over it. Whereas learning data and data in action remains Vendor assets.
• Vendor will retain the data for purposes of enforcing the Agreement, collecting fees due to Vendor, and defending against any claims and the like.

Ability to Challenge Data Accuracy.

• Data in question is data that is received from BOCES. Data will remain unmodified and unaltered. Data is mainly used to create derived anonymous metadata. Data will be available back in a simple file formats for BOCES to verify its accuracy.

Subcontractor Security Protocols.

• Vendor will treat data provided as confidential and shall protect the nature of such data by using the same degree of care, but not less than a reasonable degree of care, as we use to protect our own confidential data, so as to prevent the unauthorized dissemination or publication of provided data to third parties.
• Vendor ingests client data files via an FTP Server (provided by Files.com) which uses SSL/TLS for all communications. Each client has separate credentialed access to their private Vendor-Space on this FTP Server. Vendor pulls client files from this FTP Server over SSL/TLS encrypted connection into its AWS Virtual Private Cloud (VPC) where it is stored encrypted in S3. Once the client data arrives into our AWS VPC, it does not get copied or shared externally for any application process.

In accordance with Vendor's data security and privacy Plan, Vendor agrees that any of its officers or employees, and any officers or employees of any subcontractor or assignee of Vendor, who will have access to the shared Student Data, have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving the data or access to the data. Upon request, Vendor and/or its subcontractors or assignees will provide a certification from an appropriate officer that the requirements of this paragraph have been satisfied in full.

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

(b) 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.

(c) 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 subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(d) 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.

(e) 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 unless required by law. 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:

John Ruff
Signature

John Ruff
Printed Name

COO
Title

06-15-2020

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND MESA CLOUD INC.

Erie 1 BOCES has entered into a Master License and Service Agreement ("**MLSA**") with Mesa Cloud, Inc. ("**Vendor**") which governs the availability to Participating Educational Agencies of the following Services:

Audit services relating to student schedules and graduation requirements

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 Services 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: providing such subcontractors, assignees, or other authorized agents with such information and training as is necessary to ensure that they abide by the provisions of this Agreement.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on June 1, 2020 and expires on July 1, 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.

Supplement to