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: [Insert here – also provide a copy of Data Security and Privacy Plan]

Cengage Learning, Inc. maintains a formal, written information security program containing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personal information. This program is reasonably designed to protect (i) the security and confidentiality of personal information, (ii) protect against any anticipated threats or hazards to the security or integrity of the information, and (iii) protect against unauthorized access to or use of the information.

This document provides an overview of Cengage 's information security program.

1. Information Security Management

Cengage has established a Security Organization, led by the company's Chief Security Officer and staffed with dedicated security personnel. This organization is independent from the various divisions or business units that manage and operate IT systems within the company.

The Security Organization consists of cross-divisional security teams leveraging a multi-disciplinary approach to compliance with cyber and information security standards, operational risk management, client security management, workforce protection and business resilience. Roles and responsibilities have been formally defined in writing for all members of the security team.

2. Identification of Risks

Cengage periodically assesses the risks associated with its processing activities, including risks associated with its third-party processors, to confirm that foreseeable risks are managed properly. If a security gap is identified, new controls are agreed and defined in an agreement with such external parties.

3. Formal Definition of an Information Security Policy

Cengage has developed and documented a formal information security policy that sets out Cengage's approach to managing information security. Specific areas covered by this policy include, but are not limited to the following:

- Information security responsibilities
- Electronic communications systems
  - E-mail security
  - Instant messaging
  - Voicemail security
- Disposing of confidential information
  - Secure on-site shredding
  - Disposal and reuse of electronic media
- Data classification
- Employee monitoring and access to employees' electronic files
- Securing confidential information ("clean desk")
- Data loss prevention tools
- Client requests for information security statements and policies

- Responding to information requests / media response guidelines
- Third-party access to Cengage or client confidential information
- Mobile device management
  - Laptop security guidelines
  - Smart device guidelines
  - Employee personal device guidelines
- Virus and malware protection
- Remote access
- Wireless networking access
- Electronic incident management and handling
- Internet use and “acceptable use policy” requirements
- Internet applications and services security assessment
- Identification and authorization
  - Password standards for employees
  - Password standards for system / LAN administrators and application developers of intranet systems
  - Access control standards
  - User id standards for system / LAN administrators and intranet application developers
- Computer hardware & software management
- Encryption
- IT physical security
- Incident response, reporting and tracking policy
- Facility security
  - Emergency evacuation and assembly locations
  - Handling biochemical incidents, suspicious mail and explosives
  - Physical security
  - Security guidelines for visitors
  - Visitor security information
- HR security requirements
  - Background checks
  - Cell phones, cameras and recording devices
  - Workplace safety and weapons
  - Termination of systems access for departing employees

The Cengage Code of Ethics and Security policy document is approved by management, Cengage employees are required to acknowledge receipt and acceptance of the Cengage Code of Ethics and Security policy upon commencing work with Cengage. Policies are communicated to all employees and contractors through onboarding/new hire orientation, training classes, and distribution of policies on-line.

4. Information Security Policy Review

Cengage reviews its information security policy at least once per year or whenever there are major changes impacting the functionality of Cengage's information systems.

5. Information Security Incident Response Plan

Cengage has developed a documented methodology for responding to security incidents quickly, consistently, and effectively. Should an incident occur, a predefined team of Cengage employees will activate a formal incident response plan that addresses such areas as:

- Escalations based on the classification or incident severity
- Contact list for incident reporting/escalation
- Guidelines for initial responses and follow up with involved clients
- Compliance with applicable security breach notification laws
- Investigation log
- System recovery
- Issue resolution, reporting, and review

Cengage's policies define a security incident, incident management and all employees' responsibilities regarding the reporting of security incidents.

6. Third-Party Sub-contractors/Subprocessors

Cengage uses third-party data processors and subcontractors including for processing, hosting and storage purposes. Cengage remains responsible for the quality of the services and these sub-processors' compliance with data protection/ privacy law as it applies to data processors. Cengage is committed to working with its customers to achieve an appropriate level of transparency around its use of sub-processors.

The following entities are deemed approved as subprocessors:

- Amazon.com, Inc. (AWS - Hosting services);
- Cognizant Technology Inc. (Business processing services, e.g., call center, and hosting)
- IBM Corporation (e-commerce platform services)
- Oracle Corporation (Eloqua - Digital marketing services)
- Experian Data Quality (QAS – Address verification services)
- Informatica Corporation (Address verification services)
- CyberSource Corporation (E-commerce payment management services)

7. Audit and Assurance

- **Internal Audits and Internal Control Reports.** Cengage conducts periodic vulnerability assessments to verify the sufficiency of its security measures. Cengage also engages third party

auditors to review its security controls and may provide Client with a copy of applicable internal control reports (SOC Type II), which reports shall be classified as confidential information of Cengage.

- **Client Audits.** To the extent required by law, Cengage shall permit Client (or an independent third-party auditor for Client that is subject to confidentiality obligations) to audit Cengage's security practices relevant to Personal Data processed hereunder. Unless restricted by law, these audits are subject to the following terms:

  (i) Client audits shall take place upon thirty (30) days advance notice to Cengage. Cengage shall work with Client in good faith to provide Client with the information needed to support such audit. Client and Cengage shall mutually agree to the scope and determine the agenda of the audit in advance. The audit shall, to the extent possible, rely on certifications and audit reports or other verifications available to confirm Cengage's compliance with the applicable security requirements.

  (ii) Client may conduct a site visit of Cengage's facilities at Client's expense. Access at Cengage facilities shall be subject to Cengage's reasonable access requirements and security policies. The site visit is subject to the following conditions: (i) such site visit shall occur at a mutually agreeable time not more than once during any given calendar year; (ii) such site visit shall not unreasonably interfere with or disrupt Cengage's operations; and (iii) any third party performing such site visit on behalf of Client shall execute a nondisclosure agreement with Cengage in a form reasonably acceptable to Cengage with respect to the confidential treatment and restricted use of Cengage's confidential information, (iv) the scope of the site visit must be mutually agreed upon by the parties and shall exclude direct access to Cengage's systems, applications, network components, data center or testing of transactions.

- **Audit Findings.** If Client discovers a breach of Cengage's obligations, Client and Cengage shall work expeditiously and in good faith to agree on a plan to remediate such problems ("Remediation Plan"). Once the parties agree on a Remediation Plan, Cengage shall execute and complete the same without unreasonable delay and notify Client when such actions are completed. Notwithstanding the following, Cengage's shall have the sole discretion to determine which measures are best suitable to ensure compliance with applicable security requirements and laws.

- **Cooperation with Regulatory Audits.** Cengage shall fully cooperate with Client, at Client's expense, in connection with any governmental audit or investigation regarding Client's data or the data processing activities. (In the event that such audit or investigation is a result of Cengage's violation of applicable law, then Cengage shall be responsible for the costs and expenses or the audit or investigation).

(c)

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

(e) 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.

(f) Vendor [check one] _____will __X___will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any 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.

(g) 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.

(h) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

J Fritsch
_____
Signature

Jennifer Fritsch
Printed Name

VP Gale K12 Sales
Title

6/2/2020
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND [CENGAGE LEARNING, INC. (GALE A CENGAGE COMPANY)]

ERIE 1 BOCES HAS ENTERED INTO A MASTER LICENSE AND SERVICE AGREEMENT ("MLSA") WITH [CENGAGE LEARNING, INC. (GALE A CENGAGE COMPANY)]] WHICH GOVERNS THE AVAILABILITY TO PARTICIPATING EDUCATIONAL AGENCIES OF THE FOLLOWING PRODUCT(S):

[LIST PRODUCT(S) FROM VENDOR]
MISS HUMBLEBEES ACADEMY
GALE INTERACTIVE SCIENCE

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] A summary of Vendor's subcontractors are included in Exhibit E: Cengage Learning Information Security Program Overview. Each subcontractor is subject to a written contract containing terms materially the same as those contained herein that requires it to protect all Protected Data to which it may be exposed and comply with applicable privacy laws. Vendor may, from time to time, notify Erie 1 BOCES of new subcontractors.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on 7/1/20 and expires on 6/30/23.

- 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.