EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE
Agreement

1. **Purpose**

(a) This Exhibit supplements the CENGAGE Learning/Gale ("AGREEMENT") to which it is attached, to ensure that the AGREEMENT 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 BOCES Parents Bill of Rights for Data Security and Privacy signed by CENGAGE Learning/Gale, and the Supplemental Information about the Agreement that is required to be posted on BOCES website.

(b) To the extent that any terms contained within the AGREEMENT, or any terms contained within any other Exhibits attached to and made a part of the AGREEMENT, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that CENGAGE Learning/Gale 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 AGREEMENT, 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 AGREEMENT will have the same definition as contained within the AGREEMENT.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that CENGAGE LEARNING/GALE receives from a Participating Educational Agency pursuant to the AGREEMENT.

(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 CENGAGE Learning/Gale receives from a Participating Educational Agency pursuant to the AGREEMENT.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to CENGAGE Learning/Gale'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 CENGAGE Learning/Gale's Product pursuant to the terms of the AGREEMENT.

3. **Confidentiality of Protected Data**

(a) CENGAGE LEARNING/GALE acknowledges that the Protected Data it receives pursuant to the AGREEMENT 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) CENGAGE LEARNING/GALE 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 BOCES policy on data security and privacy

4. **Data Security and Privacy Plan**

CENGAGE LEARNING/GALE agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with BOCES Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by CENGAGE LEARNING/GALE and is set forth below.

Additional elements of CENGAGE LEARNING/GALE'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 BOCES data security and privacy policy, CENGAGE LEARNING/GALE will: take reasonable steps designed to ensure the reliability of its staff and that they are subject to a binding written contractual obligation with CENGAGE LEARNING/GALE to keep the Protected Data confidential (except where disclosure is required in accordance with mandatory applicable laws, in which case CENGAGE LEARNING/GALE shall, where practicable and not prohibited by mandatory applicable law, notify BOCES of any such requirement before such disclosure) and any other person acting under its supervision who may come into contact with, or otherwise have access to Protected Data; and require that such personnel are aware of their responsibilities under this AGREEMENT and any mandatory applicable privacy laws (or CENGAGE LEARNING/GALE's own written binding policies that are at least as restrictive as this AGREEMENT).

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the AGREEMENT, CENGAGE LEARNING/GALE will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the AGREEMENT:
A summary of CENGAGE LEARNING/GALE technical security measures are included in Exhibit 3: Cengage Learning Information Security Program Overview.

(c) CENGAGE LEARNING/GALE will comply with all obligations set forth in BOCES "Supplemental
Information about the AGREEMENT" 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, CENGAGE LEARNING/GALE has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: provide staff with appropriate privacy and security training and monitor its employees and contingent workers for compliance with the CENGAGE LEARNING/GALE privacy and security program requirements on a regular basis.

(e) CENGAGE LEARNING/GALE [*check one*] X will ____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the AGREEMENT. In the event that CENGAGE LEARNING/GALE engages any subcontractors, assignees, or other authorized agents to perform its obligations under the AGREEMENT, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in BOCES "Supplemental Information about the AGREEMENT," below.

(f) CENGAGE LEARNING/GALE will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and CENGAGE LEARNING/GALE 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) CENGAGE LEARNING/GALE will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the AGREEMENT is terminated or expires, as more fully described in BOCES "Supplemental Information about the AGREEMENT," below.

5. **Additional Statutory and Regulatory Obligations**

CENGAGE LEARNING/GALE 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 AGREEMENT 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 CENGAGE LEARNING/GALE in fulfilling one or more of its obligations under the AGREEMENT.

(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 CENGAGE LEARNING/GALE using the information to carry out

CENGAGE LEARNING/GALE's obligations under the AGREEMENT, 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 BOCES "Supplemental Information about the AGREEMENT," below.

(g) Provide notification to 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 CENGAGE LEARNING/GALE 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 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 CENGAGE LEARNING/GALE or its subcontractors or assignees.

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

(a) CENGAGE LEARNING/GALE shall promptly notify 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 CENGAGE LEARNING/GALE has discovered or been informed of the breach or unauthorized release.

(b) CENGAGE LEARNING/GALE will provide such notification to BOCES by contacting the Data Protection Officer directly by by calling (518) 862-4920 (office).

(c) CENGAGE LEARNING/GALE will cooperate with BOCES and provide as much information as possible directly to the General Counsel or designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date CENGAGE LEARNING/GALE 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 CENGAGE LEARNING/GALE 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 CENGAGE LEARNING/GALE representatives who can assist affected individuals that may have additional questions.

(d) CENGAGE LEARNING/GALE acknowledges that upon initial notification from CENGAGE LEARNING/GALE, BOCES, as the educational agency with which CENGAGE LEARNING/GALE contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New

York State Education Department ("CPO"). CENGAGE LEARNING/GALE shall not provide this notification to the CPO directly. In the event the CPO contacts CENGAGE LEARNING/GALE directly or requests more information from CENGAGE LEARNING/GALE regarding the incident after having been initially informed of the incident by BOCES, CENGAGE LEARNING/GALE will promptly inform General Counsel or designees.

(e) CENGAGE LEARNING/GALE will consult directly with the Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT ____ (CONTINUED)

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Albany-Schoharie-Schenectady-Saratoga BOCES (BOCES) is committed to protecting the privacy and security of personally identifiable information about students who attend BOCES instructional programs in accordance with applicable law, including New York State Education Law Section 2-d.

To further these goals, BOCES wishes to inform parents 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.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, 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 may be directed to the NYS Chief Privacy Officer by writing to the New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: CPO@mail.nysed.gov.

BY THE CENGAGE LEARNING/GALE:

_____
Signature

VP Gale, K12 Sales
_____
Title

5/21/2020
_____
Date

EXHIBIT ____ (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE AGREEMENT BETWEEN
Albany-Schoharie-Schenectady-
Saratoga BOCES AND CENGAGE
LEARNING/GALE

BOCES has entered into An Agreement ("AGREEMENT") with CENGAGE LEARNING/GALE ("CENGAGE LEARNING/GALE"), which governs the availability to Participating Educational Agencies of the following Product(s):

CENGAGE Learning/Gale
Exams

Pursuant to the AGREEMENT, Participating Educational Agencies may provide to CENGAGE LEARNING/GALE, and CENGAGE LEARNING/GALE 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 CENGAGE LEARNING/GALE is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above.

To be completed by CENGAGE LEARNING/GALE:

The exclusive purpose for which CENGAGE LEARNING/GALE is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. CENGAGE LEARNING/GALE agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the AGREEMENT. Protected Data received by CENGAGE LEARNING/GALE, or any of CENGAGE LEARNING/GALE'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 CENGAGE LEARNING/GALE engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (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 CENGAGE LEARNING/GALE under the AGREEMENT and applicable state and federal law. CENGAGE LEARNING/GALE will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by:
A summary of CENGAGE LEARNING/GALE subcontractors are included in Exhibit 3: 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. CENGAGE LEARNING/GALE may, from time to time, notify BOCES of new subcontractors.

Duration of AGREEMENT and Protected Data Upon Expiration:

- The AGREEMENT commences on [*date*] and expires on [*date*]. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, CENGAGE LEARNING/GALE will securely delete or otherwise destroy any and all Protected Data remaining in the possession of CENGAGE LEARNING/GALE or its assignees or subcontractors. If requested by a Participating Educational Agency, CENGAGE LEARNING/GALE will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.
- At BOCES request, CENGAGE LEARNING/GALE will cooperate with BOCES as necessary in order to transition Protected Data to any successor CENGAGE LEARNING/GALE(s) prior to deletion.
- CENGAGE LEARNING/GALE agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, CENGAGE LEARNING/GALE and/or its subcontractors, assignees, or other authorized agents will provide 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 CENGAGE LEARNING/GALE, 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 CENGAGE LEARNING/GALE by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data CENGAGE LEARNING/GALE receives will be stored on systems maintained by CENGAGE LEARNING/GALE, or by a subcontractor under the direct control of CENGAGE LEARNING/GALE, in a secure data center facility located within the United States. The measures that CENGAGE LEARNING/GALE 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: CENGAGE LEARNING/GALE (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.

Cengage Learning
Information Security Program Overview

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).