



Financial Services
Office of Procurement Services
8115 Gatehouse Road, Suite 4400
Falls Church, VA 22042

Date of Award: 7/25/2025

Cengage Learning, Inc
Attention: Jean Yacchari
5191 Natorp Boulevard
Mason, OH 45040

Reference: RFP# 2000003962 - Social Studies Basal Resource Adoption

Dear Ms. Yacchari,

Acceptance Agreement

Contract Number: 4400013782

This Acceptance Agreement signifies a contract award to Cengage Learning, Inc. for Social Studies Basal Resource Adoption for the following resources:

- *Western Civilization* (for Advanced Placement AP European History)
- *Introduction to Comparative Politics* (for Advanced Placement Comparative Government)

The period of the contract shall be from date of award through August 31, 2032 with the option to renew for three (3) additional one-year periods.

The contract award shall be in accordance with:

1. This Acceptance Agreement;
2. The Terms and Conditions of RFP 2000003962, and all addenda;
3. Your proposal signed and dated on July 7, 2024;
4. The signed Memorandum of Negotiations; and

Please note that this is not an order to proceed. A purchase order, which constitutes your notice to proceed, will be issued to your company. Please provide your Insurance Certificate according to Special Provisions Paragraph 22 within five (5) days after receipt of this letter. Contract award documents may be viewed on the Fairfax County, Department of Purchasing and Supply Management website at: www.fairfaxcounty.gov/cregister.

Sincerely,

DocuSigned by:

Michelle Pratt

611040987915402...
Michelle R. Pratt
Director

MRP/asw

Memorandum of Negotiation
4400013782
Page 2 of 8

MEMORANDUM OF NEGOTIATION

RFP# 2000003962 - Social Studies Basal Resource Adoption

The County of Fairfax, Fairfax County Public Schools (hereinafter called the County or FCPS) and Cengage Learning (hereinafter called the vendor or Cengage) hereby agree to the following in the execution of Contract 4400013782. The final contract includes and is comprised of each of the following documents (hereinafter called the Contract or the Agreement). Cengage will perform the Services in accordance with the terms and conditions set forth in the Contract. In the event of a conflict or ambiguity between or among any one or more of the contract documents listed below, and except as otherwise set forth herein, the order of precedence to be accorded such documents in resolving the conflict or ambiguity is as follows:

- a. All subsequent amendments to the contract.
- b. The Memorandum of Negotiations including the following attachments:
 1. Attachment A - Cengage Learning's Pricing Schedule
 2. Attachment B - National Data Privacy Agreement
 3. Attachment C - Cengage Learning's Service Level Agreement
- c. The following documents are incorporated by reference:
 1. Fairfax County's Request for Proposal RFP# 2000003962 - Social Studies Basal Resource Adoption and all Addenda;
 2. Cengage Learning's Technical Proposal as amended by this Memorandum of Negotiations
 3. Response to clarifications dated February 27, 2025
 4. Cengage Learning's Best and Final Offer (BAFO) dated April 2, 2025
 5. Cengage Learning's Response to IT Security Architecture Questionnaire
 6. Cengage Learning's Response to the Vendor Acceptance Questionnaire

The Parties agree that only the Director of the Office of Procurement Services may bind Fairfax County Public School Board to contract terms or conditions. Any term or condition invoked through an 'I agree' click box or other comparable mechanism (i.e., 'click wrap' or 'browse wrap' agreement) does not bind Fairfax County Public School Board or any Fairfax County Public School Board authorized end user to such terms or conditions, unless agreed to in writing by or on behalf of the Director of the Office of Procurement Services.

On April 24, 2025, at the recommendation of the negotiation team for RFP# 2000003962 - Social Studies Basal Resource Adoption, the Fairfax County School Board approved the following Cengage titles:

- *Western Civilization Since 1300 Enhanced AP Edition* (for Advanced Placement AP European History)
- *Introduction to Comparative Politics* (for Advanced Placement Comparative Government)

The parties agree to the to the following:

Memorandum of Negotiation

4400013782

Page 3 of 8

1. Exceptions to the RFP terms and conditions:

Below are the revisions made to Appendix A, General Conditions and Instructions to Bidders.

a. Section 58 a-c., Indemnification, shall revised as follows:

Indemnification. Contractor shall indemnify, defend, and hold harmless County and its respective officers, directors, employees and agents (excluding insurance carriers) ("County Indemnified Parties") from and against any claims, demands, proceedings, investigations, or suits, brought by a third party (a) to the extent arising from bodily injury, death, or damage to real or personal property caused by Contractor's negligence or willful misconduct; or (b) alleging that the Contractor materials as delivered infringe a valid United States copyright, patent, trademark, or other proprietary right (each, a "Claim Against County"). Contractor will indemnify County Indemnified Parties for any finally awarded damages or settlement amount approved by Contractor in writing to the extent arising from a Claim Against County. Notwithstanding the foregoing, Contractor shall have no obligation to indemnify County to the extent a Claim Against County arises from (a) County's use of the Contractor materials in combination with technology or services not provided by Contractor, if the alleged infringement would not exist without such combination; (b) any County content or data input into the Contractor materials, if the alleged infringement would not have occurred without input of such content or data into the Contractor materials; (c) Contractor's compliance with designs, specifications, or instructions provided in writing by County, if such infringement would not have occurred but for such designs, specifications, or instructions; or (d) use of the Contractor materials by County after notice by Contractor to discontinue use. Contractor's obligation to indemnify is contingent on County: (a) promptly providing written notice of the claim to Contractor; (b) giving Contractor sole control of the defense and settlement of the claim (provided that any settlement unconditionally releases County of all liability and does not make any admissions on behalf of County or include payment of any amounts by County); and (c) providing Contractor, at Contractor's expense, all reasonable assistance in connection with such claim. County may participate in the defense of the claim at its sole cost and expense. This paragraph sets forth Contractor's sole liability to, and County's exclusive remedy for, any Claim Against County.

b. Limited Liability shall be revised as follows:

Limited Liability. NOTWITHSTANDING ANYTHING HEREIN THE CONTRARY, THERE IS NO LIMITATION ON THE LIABILITY ON OUR PART FOR: (A) CLAIMS FOR BODILY INJURY, INCLUDING DEATH, AND DAMAGE TO REAL PROPERTY OR TANGIBLE PERSONAL PROPERTY RESULTING FROM OUR NEGLIGENCE OR THE NEGLIGENCE OF ANY EMPLOYEE; OR (B) THE INTENTIONAL OR WILLFUL MISCONDUCT, FRAUD, OR RECKLESSNESS ON OUR PART OR ON THE PART OF ANY EMPLOYEE. The following shall not apply to damages or liability resulting from third party claims or obligations arising out of bodily injury, death, or damage to property of District. Neither party nor its suppliers, nor their respective directors, employees, officers, or representatives will be liable for any damages of any kind arising from the use of or inability to use the materials, including but not limited to, any direct, indirect, incidental, special, consequential, exemplary, or punitive damages, or any lost profits, lost data, or loss of revenue. Without limiting the foregoing, either party's total liability will

Memorandum of Negotiation
4400013782
Page 4 of 8

at all times be limited to two times the fees paid by District for use of the materials at issue during the immediately preceding twelve (12) month period.

2. Accessibility:

- a. Cengage confirms their digital learning resource with alternative formats may be found here https://cengage.widen.net/s/fcbznrvzw/cengage_mtk12_vpat
- b. The vendor agrees to accessibility features requested by FCPS to be made by April 1, 2026, in compliance with the WCAG 2.1 AA. This includes but it not limited to:
 - a. Headings and labels
 - b. ReadSpeaker reads an entire page.
 - c. All video media within the platform contains accurate captions and transcripts or the platform is compatible with third party live caption tools.
 - d. All text fields within the platform can be filled using multiple inputs such as a keyboard, speech recognition, and other assistive technology.

c. As per revised Americans with Disabilities Act (ADA) Title II 28 CFR Part 35, all contracted vendors of web and mobile products are required to inform FCPS of their compliance with Web Content Accessibility Guidelines (WCAG) 2.1 by providing a Voluntary Product Accessibility Template (VPAT) annually. Cengage covenants and agrees that the Services will comply with WCAG. 2.1 as of the effective date of this Contract and that the Services will remain in compliance with WCAG 2.1 throughout the term this Contract. Cengage will promptly notify FCPS in writing if at any time during the term the Services do not comply with WCAG 2.1. FCPS reserves the right to terminate and receive a refund of prepaid amounts relating to the period following termination AND a right to indemnification from Cengage for losses, damages, penalties incurred by FCPS that arise from or in connection with the Cengage's failure to comply with the WCAG 2.1 standard.

3. Information Technology

- a. If a new platform is released during the contract period, it will be provided at no cost to FCPS. Cengage agrees to provide FCPS a minimum of six months' advance notice for a change in digital platform and will work with FCPS on a transition.
- b. Cengage agrees to provide teachers and content points of contact with early access to its platform and 'sandbox' accounts so teachers can begin setting up and planning.

4. Service Level Agreement

- a. Cengage guarantees a minimum of 99.99% availability, computed based 24 hours day over a 30-day period and outside of regularly scheduled maintenance and/or update windows. Cengage shall provide technical support at (888) 915-3276, Monday to Friday, from 8:00 AM to 7:00 PM ET (excluding national/federal holidays referenced below).

January 20th - Martin Luther King, Jr. Day Observed
February 17th - Presidents' Day Observed
May 26th - Memorial Day Observed
June 19th - Juneteenth Observed
July 4th - Independence Day Observed
September 1st - Labor Day Observed

Memorandum of Negotiation

4400013782

Page 5 of 8

November 11th - Veterans Day Observed Early close Wednesday
 November 26th - November 27th - November 28th - Thanksgiving Observed
 December 24th - January 1st - Winter Break Observed

- b. The Digital Support Portal at <https://ngl.cengage.com/resources/support> offers on-demand training, how-to guides, videos, platform-specific training, and more.

Technical point of contact
 Ator Foster, Senior Manager
 Cengage Digital Solutions
ator.foster@cengage.com
 248-699-8623

- c. Response and Resolution Turnaround time

Cengage Incident Priority, Description, and Response Table

Incident Priority	Incident Description	Incident Response Service Level
1	Service is down or unavailable	Licensors shall provide status updates every 60-90 minutes thereafter unless a difference. The cadence of updates is mutually agreed upon on a per-incident basis. Licensors will use commercially reasonable efforts to commence efforts to fix such Priority 1 Incident within 1 hour after such notification of the Incident.
2	Service functionality is substantially impacted, or significant Service performance Degradation is experienced with a high impact on business operations	Licensors shall provide status updates every 4 hours thereafter unless a different cadence of updates are mutually agreed upon on a per incident basis. Licensors will use commercially reasonable efforts to commence efforts to fix such incident within 4 hours after such notification of such Incident.
3	There is a partial, non-critical impact on Service functionality or Service performance degradation with low impact to district business operations	Licensors shall provide status updates every 24 hours thereafter unless a different cadence of updates are mutually agreed upon on a per incident basis. Licensors will use commercially reasonable efforts to commence efforts to fix such Priority 3 Incident within 72 hours after such notification of the Incident.
4	Request for a new service Requests involving routine technical issues Inquiries regarding Service capabilities Notice of minor Service performance issues for which a fix or workaround is available	Licensors will respond and/or resolve as soon as possible or within a timeframe as mutually agreed upon on a per-incident or request basis.

Support request escalation (when a request severity level increases). Cengage has a structured support request escalation process to ensure the timely resolution of issues based on severity.

- Low Severity: Minor issues that do not significantly impact usage.
- Medium Severity: Issues that affect functionality but have workarounds.

Memorandum of Negotiation

4400013782

Page 6 of 8

- High Severity: Critical issues that severely impact usage and have no immediate workaround.

d. Scheduled Maintenance

General maintenance shall be performed as needed to support, address any bugs or implement scheduled changes to the platform. The maintenance window shall be off-hours to the greatest extent possible and will not require any downtime.

Scheduled maintenance or downtime within operational hours (8 a.m. – 5 p.m. ET) must be communicated to Rick Mayfield at rmayfield@fcps.edu or any FCPS appointment designee 5 days prior to the event.

5. Cultural Responsiveness

- a. For content issues identified by FCPS, Cengage agrees to work alongside FCPS to find solutions. Cengage will take 4 to 6 weeks to review the request, consult with the subject matter experts, and assess the most effective and least disruptive way to represent the requested changes.

6. Curriculum

- a. Cengage will collaborate with FCPS to develop a process for reviewing requests, agreeing on changes, and determining the format of delivery (e.g., digital only, with no updates to print). These revisions will be reviewed on a case-by-case basis to assess scope, timing, and resource availability.
- b. The vendor shall provide eBook content that is compatible with Google Translate.
- c. If FCPS discovers any factual or editing errors, the vendor shall review in a timely manner and partner with FCPS on resolution.
- d. The vendor shall deliver professional development at no cost to FCPS:
 - July - August 2025: synchronous webinars
 - August 13, 2025: synchronous pre-service
 - September 19, 2025: virtual
 - October 13, 2025: synchronous in-service
 - November 3, 2025 synchronous in-service
 - December 2025: virtual synchronous
 - January 30, 2026: synchronous in-service
 - February 17 & 20, 2026: synchronous in-service.

Vendor agrees to deploy trainers familiar with multilingual learners and special education students to support teacher training. Training in Years 2-7 of the implementation will be mutually agreed upon with FCPS and vendor. Additional on-site professional development will be provided to FCPS at the rate of \$1,500 per day.

7. Pricing/Shipping

- a. Vendor agrees to deliver print materials directly to schools with a list of points of contact, addresses, and numbers provided by FCPS. Delivery trucks shall have lift gates to ensure inside delivery for schools without loading docks. Deliveries shall be palletized by school with ISBN Numbers as well as titles to allow for ease of product verification.

Memorandum of Negotiation

4400013782

Page 7 of 8

- b. Vendor agrees to a shipping fee of 5% of the purchase price for year 1 for print resources. A 2.5% shipping/processing fee for all subscription purchases (co-terminus contracts) that are purchased within the 7-year contract period will be applied.
- c. Delivery Dates can be negotiated with individual schools based on PO acceptance. If not received at the negotiated date, the vendor will provide a rebate of 1% of the purchase value of resources not delivered on time.

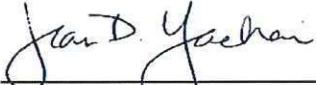
8. Performance Metrics

Performance Metric & Description	Target	Data Source	Data Collection Frequency
100% compliance with the WCAG 2.1 AA initially by April 1, 2026 and ongoing from that point on	Compliance with Title II ADA	VPAT on each product ACR for each product	Annually in July and upon any changes to features Within 45 days of contract signing
100% of files will be uploaded into NIMAC within 45 days from Date of Award	Student accessibility	NIMAC files	Verified 45 days from Date of Award and annually
Usage reports by student, teacher, school, and course provided to FCPS POC via the learning platform	Product availability and accessibility	Reports	Within 10 business days of the end of each FCPS quarter
High quality professional development to support implementation and ongoing usage of Cengage selected products	80% or more of attendees reporting high or moderately high levels of satisfaction at all in-person training provided by Cengage	Summary of post-training surveys	Within five days of each in-person training event.
Monthly and responsive (within 2 days of outreach) communication between vendor and assigned FCPS point of contact	FCPS assigned POC is fully aware of product issues and updates and inquiries from FCPS staff	Quarterly feedback	Within 10 business days of the end of each FCPS quarter

Contractor agrees that it will (a) comply with all laws, rules, and regulations applicable to the Services provided hereunder; and (b) will maintain throughout the term of this Agreement the same or functionally-equivalent or substantially similar (or more stringent) practices, procedures, methodologies, and certifications as are described in its completed Security Architecture Questionnaire and Vendor Acceptance Questionnaire (the "Security Practices") which is incorporated herein by reference, except if required by law or reasonable business need. All other prices, terms, and conditions remain the same.

Memorandum of Negotiation
4400013782
Page 8 of 8

ACCEPTED BY:



Jean Yacchari
Cengage Learning, Inc

06/17/2025

Date



Noel Klimenko, Assistant Superintendent
Instructional Services FCPS
DocuSigned by:

June 24, 2025

Date



C14D4C9B7D1F422...
Michelle R. Pratt, Director
Office of Procurement Services

7/25/2025

Date

PLEASE NOTE:
If the "Digital" column is marked, indicate length of subscription (in years) included with purchase in the "Subscription Length" column
If a bundle is submitted as a line item below, provide comprehensive information describing which items are included in the bundle (use additional documentation if necessary)
If a line item may be offered gratis, indicate that in the "Gratis" column and provide details elsewhere describing terms of discount
Additional documentation can be used to provide more information for line items, if necessary. Please indicate on any additional documentation to which line item it refers.
If a line item may be offered gratis, please indicate in the "Gratis" column and provide details elsewhere describing terms of discount.

RFP 2000003962
Appendix E - Pricing Schedule
Vendor Name: National Geographic Learning | Cengage

								Mark all that apply				
Line Item #	FCPS Course Name (Course List Line Number, Ref: Attachment A Social Studies Course List)	ISBN	Textbook Title	Author(s)/ Editor(s)	Edition	Copyright Year	UOM	Print	Digital	Subscription Length (Years)	Contract Price	Gratis (Y/N), provide details
16	AP U.S. Government	9780357541586	American Government Institutions and Policies	Wilson/Dilulio, Jr/Bose/Levendusky	16th	2022		X			174.25	
17	AP U.S. Government	9780357578353	American Government Bundle: Print/MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th	2022		X	X	1	182.25	
	AP U.S. Government	9780357544914	American Government: MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th				X	1	50	
	AP U.S. Government	9780357866030	American Government: MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th				X	2	75	
	AP U.S. Government	9780357866047	American Government: MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th				X	3	100	
	AP U.S. Government	9798214155036	American Government: MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th				X	4	120	
	AP U.S. Government	9780357870969	American Government: MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th				X	5	145	
	AP U.S. Government	9780357544907	American Government: MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th				X	6	169	
18	AP U.S. Government	9780357995495	American Government Bundle: Print/MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th	2022		X	X	7	217.5	
19	AP U.S. Government	9780357544914	American Government MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th	2022			X	1	50	
20	AP U.S. Government	9798214077390	American Government MindTap	Wilson/Dilulio, Jr/Bose/Levendusky	16th	2022			X	7	199	
21	AP U.S. Government	9780357544976	Fast Track to a 5 Test Prep for American Government Institutions and Policies	Wilson/Dilulio, Jr/Bose/Levendusky	16th	2022		X			27.25	
22	AP European History	9780357433379	Western Civilization Since 1300 Enhanced AP Edition	Spielvogel	10th	2021		X			148.75	
23	AP European History	9780357491782	Western Civilization Bundle: Print/MindTap	Spielvogel	10th	2021		X	X	1	156.75	
24	AP European History	9780357780190	Western Civilization Bundle: Print/MindTap	Spielvogel	10th	2021		X	X	7	192	
25	AP European History	9780357433393	Western Civilization MindTap	Spielvogel	10th	2021			X	1	50	
	AP European History	9780357922903	Western Civilization MindTap	Spielvogel	10th	2021			X	2	70	
	AP European History	9780357545928	Western Civilization MindTap	Spielvogel	10th	2021			X	3	90	
	AP European History	TBD	Western Civilization MindTap	Spielvogel	10th	2021			X	4	120	
	AP European History	9780357877333	Western Civilization MindTap	Spielvogel	10th	2021			X	5	130	
	AP European History	9780357437803	Western Civilization MindTap	Spielvogel	10th	2021			X	6	149	
26	AP European History	9780357997413	Western Civilization MindTap	Spielvogel	10th	2021			X	7	168.5	



STANDARD STUDENT DATA PRIVACY AGREEMENT

(National Data Privacy Agreement (NDPA) Standard VERSION 2)

Fairfax County School Board

And

Cengage Learning, Inc.

Version 2

Authored by Members of the Student Data Privacy Consortium (SDPC) &

Mark Williams, Fagen, Friedman & Fulfrost LLP

© Access 4 Learning (A4L) Community. All Rights Reserved.

This document may only be used by A4L Community members and may not be altered in any substantive manner.

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “Effective Date”) and is entered into by and between:

Fairfax County School Board, the public body in Virginia that operates Fairfax County Public Schools,

located at Office of Procurement Services – Gatehouse Administration Center at 8115 Gatehouse Road, Suite 4400, Falls Church, VA 22042-1203 (the “LEA”)

and

Cengage Learning, Inc. located at 5191 Natorp Blvd. Mason, OH 45040 (the “Provider”).

PREAMBLE

WHEREAS, the Provider is providing educational or digital Services, as defined in Exhibit “A”, to LEA, which Services may include: (a) cloud-based Services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA have entered into a Service Agreement (as defined herein), to provide certain Services to the LEA as set forth in the Service Agreement, and this DPA (collectively the “Agreement”),

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment (“PPRA”) at 20 U.S.C. 1232h; and the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. 6501-6506 (16 C.F.R. Part 312),

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

Special Provisions. (Check if Required)

☐ If checked, the Provider has signed Exhibit “E” to the SDPC Standard Clauses, otherwise known as “General Offer of Privacy Terms” enabling other LEAs to enter into the same terms of this DPA with Provider.

☒ If checked, the Supplemental State Terms attached hereto as Exhibit “G” are hereby incorporated by reference into this DPA in their entirety.

If the Parties desire to change any terms, use the ‘Vendor-Specific’ Agreement or ‘District-Modified’ Agreement.

STANDARD STUDENT DATA PRIVACY AGREEMENT

Version 2.0

The **designated representative for the LEA** for this DPA is:

Name: Michelle Pratt Title: Director, OPS
Address: 8115 Gatehouse Rd. Suite 4400 Falls Church, VA 22042
Phone: 571-423-3555 Email: mrpratt@fcps.edu

The **designated representative for the Provider** for this DPA is:

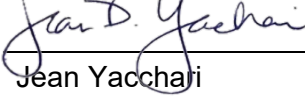
Name: Jean Yacchari Title: K12 Contracts Program Manager
Address: 5191 Natorp Boulevard, Mason, Ohio 45040
Phone: 513-630-8251 Email: jean.yacchari@cengage.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Fairfax County School Board

Signed By:  Date: 4/11/2025 | 1:57 PM EDT
Printed Name: Michelle Pratt Title/Position: Director, Office of Procurement Svcs

PROVIDER: Cengage Learning, Inc.

Signed By:  Date: 03/10/2025
Printed Name: Jean Yacchari Title/Position: K12 Contracts Program Manager

Each Party is responsible to promptly notify the other Party of changes to the notice information.

Notices to Provider

[Adrienne Wells]
[Institutional Account Rep]
[5191 Natorp Blvd., Mason OH 45040]
[adrienne.wells@cengage.com]

Notices to LEA

Michelle R. Pratt
OPS Director
8115 Gatehouse Rd. Suite 4400 Falls Church, VA 22042
mrpratt@fcps.edu

With a copy to (if provided):

[Provider Legal Counsel]
[5191 Natorp Blvd., Mason OH 45040]
[privacy@cengage.com]

With a copy to (if provided):

Fairfax County Public Schools, Office of Division
Counsel
8115 Gatehouse Road, Falls Church, VA 22042-1203

Security Notices to Provider (Required per Section 5.3)

[Desarie Green]
[Sr. Privacy Counsel]
[5191 Natorp Blvd., Mason OH 45040]
[privacy@cengage.com]

Security Notices to LEA (Required per Section 5.3)

Taniko Lowman
Senior Manager, Security Architecture
3701 Franconia, Rd. Alexandria, VA 22310
tnlowman@fcps.edu

STANDARD CLAUSES

ARTICLE I: PURPOSE AND SCOPE

1.1 Purpose of DPA.

The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing Services otherwise provided by the LEA. With respect to its use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA as set forth in this DPA and the Service Agreement, or by executing an amendment with the LEA.

1.2 Description of Products and Services.

A description of all products and services covered by the Agreement, and information specific to this DPA, are listed in Exhibit "A". If a Provider needs to update any information on Exhibit "A" (such as updating with new provided services), they may do so by completing the Addendum template provided by the A4L Community and sending a copy to the LEA.

Provider may add or delete products or services subject to this DPA under the following circumstances:

1. Deleted products or services: The products or services have been discontinued and are no longer available from the Provider.
2. Added products or services: The added products or services are either:
 - a. a direct replacement, or substantially equivalent to the original products or services listed in the DPA
 - b. the added products or services result in enriched new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed, or
 - c. the LEA elects to subscribe to additional or different products or services after the DPA was signed, in which case the Provider and the LEA shall enter into an amendment with respect to such additional products or services.

If an added product or service requires additional Data Elements, Provider must complete the relevant portion of the Addendum template to update Exhibit "B".

Provider may not make any change to Exhibit "A" via an Addendum, except adding or deleting products or services. LEA is under no obligation to acquire added products or services, and has no ability under the DPA to prevent deletion of products or services. Subject to the limitations in this section, an Addendum is automatically incorporated into this DPA when LEA is notified by Provider, in accordance with the notification provisions of this DPA, of the Addendum's existence and contents.

1.3 Student Data to Be Provided.

In order to perform the services, the Provider shall process Student Data as identified by the Provider in the Schedule of Data, attached hereto as Exhibit "B". Student Data may be provided by the LEA or created by students, as set forth fully in the definition of Student Data in Exhibit "C". If a Provider needs to update any

information on Exhibit “B”, they may do so by completing the Addendum template provided by the A4L Community and sending a copy to the LEA.

Provider may delete data elements from Exhibit “B” if they are no longer used by the Provider.

Provider must add data elements to Exhibit “B”, when a material change has occurred, regardless of whether the added data elements are either one of the following:

1. used to better deliver the original products or services listed in the DPA, or
2. used to deliver added products or services that result in new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed. Such new products or services must be designated in the Addendum template as changes to Exhibit “A”.

The Provider must notify the LEA, in accordance with the notification provisions of this DPA, of the existence and contents of an Addendum modifying Exhibit “B”. The LEA will have thirty (30) days from receipt to object to the Addendum. If no written objection is received it will become incorporated into the DPA between the parties.

1.4 DPA Definitions.

Capitalized terms used in this DPA shall have the meanings set forth in Exhibit “C”. With respect to the treatment of Student Data, in the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to, the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1 Student Data Property of LEA.

As between LEA and Provider, all Student Data processed by the Provider, or created by students (as set forth fully in the definition of Student Data in Exhibit “C”), pursuant to the Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data processed by the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA.

2.2 Parent, Legal Guardian and Student Access.

The LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student (as defined in FERPA) may review Student Data and request deletion or modification, and request delivery of a copy of the Student Data. Provider shall respond in a reasonably timely manner (and no later than thirty (30) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent, legal guardian or student, whichever is sooner) to the LEA’s request for Student Data held by the Provider to view or correct as necessary.

In the event that a parent or legal guardian of a student or eligible student contacts the Provider to correct, delete, review or request delivery of a copy of any of the Student Data collected by or generated through the Services, the Provider shall refer that person to the LEA, who will follow the necessary and proper procedures regarding the requested information. In the event that any person other than those listed contacts the Provider about any Student Data, the Provider shall refer that person to the LEA, except as provided in Section 4.4.

- 2.2.1 This NDPA does not impede the ability of students to download, export, or otherwise save or maintain their own Student Generated Content directly from Provider or for Provider to provide a mechanism for such download, export, transfer or saving to students, or the student's parent or legal guardian. Nor does it impede the ability of Providers to offer LEAs features to allow such ability.
- 2.2.2 In the event that Student Generated Content is transferred to the control of the student, parent or legal guardian, the copy of such Student Generated Content that is in the control of such person is no longer considered Student Data.

2.3 Subprocessors.

Provider shall enter into a Subprocessor Agreement with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner not materially less stringent than the terms of this DPA. Every Subprocessor Agreement must provide that the Subprocessor will not Sell the Student Data. The terms of a Subprocessor Agreement shall not be materially modified by the Subprocessor unless notice is provided to the Provider.

ARTICLE III: DUTIES OF LEA

3.1 Provide Data in Compliance with Applicable Laws.

LEA shall use the Services and provide Student Data in compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time. To the extent the Services involve the collection by the Provider of personal information (as such term is defined in the Children's Online Privacy Protection Act) from children under the age of thirteen (13), the LEA consents on behalf of parents to the collection of personal information for education purposes that benefit the LEA and not for other commercial purposes. The LEA authorizes the collection of personal information. The Provider's privacy notices are available at <https://www.cengagegroup.com/privacy/>.

3.2 Annual Notification of Rights.

If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.

3.3 Reasonable Precautions.

LEA shall employ administrative, physical, and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted Student Data from unauthorized access, disclosure, or acquisition by an unauthorized person.

3.4 Unauthorized Access Notification and Assistance.

LEA shall notify Provider within seventy-two (72) hours of any confirmed Data Breach to the Services, LEA's account or any Student Data that poses a privacy or security risk. If requested by Provider, LEA will provide reasonable assistance to Provider in any efforts by Provider to investigate and respond to such Data Breach.

ARTICLE IV: DUTIES OF PROVIDER

4.1 Privacy and Security Compliance.

The Provider shall comply with all laws and regulations applicable to Provider's protection of Student Data privacy and security, and upon written request of the LEA shall reasonably cooperate with any state or federal government initiated audit of the LEA's use of the Services.

4.2 Authorized Use.

The Student Data processed pursuant to the Services shall be used by the Provider for no purpose other than performing the Services outlined in Exhibit "A" or stated in the Service Agreement or this DPA, as instructed by the LEA, or as otherwise required by law.

4.3 Provider Employee Obligation.

Provider shall require all of Provider's employees who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee with access to Student Data pursuant to the Service Agreement.

4.4 No Disclosure.

Provider acknowledges and agrees that it shall not sell or disclose any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data.

4.4.1 Exceptions to No Disclosure.

- 4.4.1.1 This prohibition against disclosure will not apply to Student Data where disclosure is directed or permitted by the LEA or this DPA.
- 4.4.1.2 The provision to not sell Student Data shall not apply to a Change of Control.
- 4.4.1.3 This prohibition against disclosure shall not apply to Student Data disclosed pursuant to a judicial order or lawfully issued subpoena or warrant.
- 4.4.1.4 This prohibition against disclosure shall not apply to Student Data disclosed to Subprocessors performing Services on behalf of the Provider pursuant to this DPA.
- 4.4.1.5 Should law enforcement or other government entities ("Requesting Party(ies)") provide a judicial order or lawfully issued subpoena or warrant to the Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party.
- 4.4.1.6 Notification under 4.4.1.5 is not required if the judicial order or lawfully issued subpoena or warrant states not to inform the LEA of the request.
- 4.4.1.7 Should the LEA be presented with a judicial order or lawfully issued subpoena or warrant to disclose Student Generated Content or other Student Data, the Provider shall reasonably cooperate with the LEA in delivering such data.

- 4.4.1.8 This prohibition against disclosure shall not apply to LEA-authorized users of the Services, which may include parents and legal guardians.
- 4.4.1.9 This prohibition against disclosure shall not apply to protect the safety of users or others, if and only if, an LEA employee who has specifically been authorized to declare a health or safety emergency has done so and all requirements under 34 CFR §§ 99.31(a)(10) and 99.36 have been fulfilled by the LEA.
- 4.4.1.10 This prohibition against disclosure shall not apply to protect the integrity or security of the Service, where such disclosure is made to a Subprocessor engaged by Provider for the specific purpose of investigating a potential Data Breach as set forth in 5.4.

4.5 De-Identified Data

Provider agrees not to attempt to re-identify De-Identified Student Data without the written direction of the LEA. De-Identified Student Data may be used by the Provider for those purposes allowed under applicable laws, for the purposes allowed for the processing of Student Data under this DPA, as well as the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) research, development, and improvement of the Provider's educational sites, Services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Student Data shall survive termination of this DPA or any request by LEA to return or dispose of Student Data. Except for Subprocessors, Provider agrees not to transfer De-identified Student Data to any third party unless that party agrees not to attempt reidentification in writing and is subject to terms not materially less protective than the terms of this DPA. Such Subprocessors must be subject to terms not materially less protective than the terms of this DPA. Prior to publishing any document that names the LEA, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Student Data is presented. If Provider chooses to create De-Identified Data, its process must comply with either NIST de-identification standards or US Department of Education guidance on de-identification.

4.6 Disposition of Data.

Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree.

If the Provider has a standard retention and destruction schedule, that schedule shall apply to Student Data as long as this DPA is active. A summary of the Provider's practices relating to retention and disposition of Student Data shall be provided to the LEA upon written request.

At the termination of this DPA, the Provider shall, unless directed otherwise by the LEA, dispose of, or delete Student Data obtained by the Provider under the Agreement within sixty (60) days of termination (unless otherwise required by law, provided that the terms of this DPA shall survive and apply with respect to such retained data and Provider shall only use and disclose the retained data for the purposes that require its retention). If the Agreement has lapsed or is not terminated, the Student Data shall be deleted when directed or permitted by the LEA, according to Provider's standard destruction schedule, or as otherwise required by law. The LEA may provide the Provider with special instructions for the disposition of the Student Data, by transmitting to Provider Exhibit "D", attached hereto. The duty of the Provider to dispose of or delete Student Data shall not

extend to De-Identified Data or to Student-Generated Content that has been transferred or kept pursuant to Section 2.2.2.

4.7 Advertising Limits.

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA; or (c) for any commercial purpose other than to provide the Service to the LEA, or as authorized by the LEA or the parent/guardian. Targeted Advertising is strictly prohibited. However, this section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or other LEA employees that are not considered Targeted Advertising ; or (iii) to notify account holders about new education product updates, features, or Services that are not considered Targeted Advertising or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA SECURITY AND BREACH PROVISIONS

5.1 Data Storage.

If Student Data is stored outside the United States, Provider will provide a list of Countries where data is stored, in Exhibit “B”.

5.2 Security Audits.

Provider will conduct a security audit or assessment no less than once per year, and upon a Data Breach. Upon 15 days’ written notice and execution of confidentiality agreement, Provider will provide the LEA with a copy of a commercially reasonable summary, subject to reasonable and appropriate redaction.

5.3 Data Security.

The Provider agrees to utilize reasonable administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security of Student Data. The Provider shall implement an adequate Cybersecurity Framework that incorporates one or more of the nationally or internationally recognized standards set forth in Exhibit “F”. Additionally, Provider may choose to further detail its security programs and measures in Exhibit “F”. Provider shall provide, in the Preamble to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

5.4 Data Breach.

In the event that Provider confirms a Data Breach, the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the Data Breach, unless notification within these time limits would disrupt investigation of the Data Breach by law enforcement. In such an event, notification shall be made within a reasonable time after the Data Breach. Provider shall follow the following process:

- (1) The Data Breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - (a) The name and contact information of the Provider subject to this section,
 - (b) the date of the notice,

- (c) the date of the Data Breach, the estimated date of the Data Breach, or the date range within which the Data Breach occurred,
 - (d) Whether the notification was delayed as a result of a law enforcement investigation, if legally permissible to share that information,
 - (e) A general description of the Data Breach, if that information is possible to determine at the time the notice is provided,
 - (f) A description of the Student Data reasonably believed to have been the subject of the Data Breach; and
 - (g) Identification of impacted individuals.
- (2) Provider agrees to adhere to all applicable federal and state laws with respect to a Data Breach related to the Student Data, including any required responsibilities and procedures for notification and mitigation of any such Data Breach.
- (3) Provider further acknowledges and agrees to have a written Data Breach response plan that is consistent with applicable industry standards and federal and state law for responding to a Data Breach, involving Student Data and agrees to provide LEA, upon reasonable written request, with a summary of said written Data Breach response plan.
- (4) LEA shall provide notice and facts surrounding the Data Breach to the affected students, parents, or guardians.
- (5) In the event of a Data Breach originating from LEA's use of the Service or otherwise a result of LEA's actions or inactions, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data and may request costs incurred as a result of such Data Breach.

CONTRACT TERMS

Term and Termination. In the event that either Party seeks to terminate this DPA, they may do so by written notice if the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any Service Agreement or contract if the other party materially breaches any terms of this DPA, provided that the other Party has been given notice of such breach and has had a reasonable period of time, but in no event less than thirty (30) days, to remedy such breach prior to termination. This DPA shall stay in effect for as long as the Provider retains the Student Data, as set forth in section Article IV, Section 4.6. In the case of a “Change of Control” the LEA has the authority to terminate the DPA if it reasonably believes that the successor cannot uphold the terms and conditions herein or having a contract with the successor would violate the LEA’s policies or state or federal law.

Data Disposition on Service Agreement Termination. If the Service Agreement is terminated, the Provider shall dispose of all of LEA’s Student Data pursuant to Article IV, Section 4.6 of the Standard Clauses.

Notices. All notices or other communication required or permitted to be given hereunder must be made in writing and may be given via e-mail transmission, or first-class mail, or mutually agreed upon method sent to the designated representatives documented in the Preamble.

Priority of Agreements. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. With respect to the treatment of Student Data only, in the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit “H”, the SDPC Standard Clauses, and/or the Supplemental State Terms in Exhibit “G”, Exhibit “H” will control, followed by Exhibit “G”. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

Entire Agreement. This DPA and the Service Agreement (“the Agreement”) constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties.

Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

Governing Law; Venue and Jurisdiction. This DPA will be governed by and construed in accordance with the laws of the state of the LEA, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction to the state and federal courts for the county of the LEA for any dispute arising out of or relating to this DPA or the transactions contemplated hereby.

Successors Bound. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a Change of Control. In the event of a Change of Control, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of such Change of Control. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement.

Authority. Each signatory confirms they are authorized to bind their institution to this DPA in its entirety.

Waiver. No delay or omission by either party to exercise any right here under shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

Limitation of Liability. NOTWITHSTANDING ANYTHING IN THE SERVICE AGREEMENT OR THIS DPA TO THE CONTRARY, AND EXCEPT FOR GROSS NEGLIGENCE AND WILLFUL MISCONDUCT, PROVIDER'S LIABILITY SHALL NOT EXCEED THE FEES PAID BY LEA IN CONNECTION WITH THE PROVISION OF THE SERVICES UNDER THE SERVICE AGREEMENT DURING THE TWENTY-FOUR (24) MONTHS PRECEDING THE EVENT GIVING RISE TO THE LIABILITY. IN NO EVENT SHALL PROVIDER BE LIABLE TO LEA IN ANY RESPECT, FOR INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL OR PUNITIVE DAMAGES, ARISING OUT OF THE SERVICE AGREEMENT OR THIS DPA OR THE ACTS OR OMISSIONS IN FULFILLING ITS OBLIGATIONS HEREUNDER. Notwithstanding the foregoing, there is no limitation of liability of Provider for: (a) claims for bodily injury, including death, and damage to real property or tangible personal property resulting from the negligence of Provider or any employee of Provider; or (b) the intentional or willful misconduct, fraud, or recklessness of Provider or any employee of Provider.

EXHIBIT A: PRODUCTS AND SERVICES

This DPA covers access to and use of Cengage Learning, Inc.'s existing Services that collect, process, or transmit Student Data, as identified below:

Unless specified, and explicitly excluded below, this DPA covers access to and use of all Cengage Learning, Inc.'s Services, as well as any future Services that Cengage Learning, Inc. may offer. This coverage extends, without limitation, to all subdomains, software, mobile applications, and products that are owned and operated by Cengage Learning, Inc., its subsidiaries, and/or affiliates, except for those explicitly excluded below. If applicable, any EXCLUDED services will be listed below and are therefore not covered by this DPA:

EXHIBIT B: SCHEDULE OF STUDENT DATA

All Data Elements identified in this Exhibit are correct at time of signature.

Data Elements Collected by Product (required and optional):

Category of Data Data Elements	Omni Platform	Mindtap, Mindtap School	CNOWv2, OWLv2, Webassign	Ed2go	CIMA	Spark	PRODUCT NAME(S)
Application Technology MetaData							
IP Addresses of users, use of cookies, etc.		MT	CNOW, OWL, WA	X	X	X	
Other application technology metadata			CNOW, OWL, WA		X		
If 'Other' checked, please specify below checked box:			Browser name/ version/ type		Browser or device use		
Application Use Statistics							
Metadata on user interaction with application		MTS, MT	CNOW, OWL, WA	X	X		
Assessment							
Standardized test scores			CNOW, OWL				
Observation data			CNOW, OWL				
Other assessment data			WA		X		
If 'Other' checked, please specify below checked box:			Time Accomodation		Scores and grades of quizzes and other assignment types		
Attendance							
Student school (daily) attendance data	X				X		
Student class attendance data				X	X		
Communication							
Online communication captured (emails, blog entries)	X		CNOW, OWL, WA	X	X	X	
Conduct							
Conduct or behavioral data			CNOW, OWL				
Demographics							
Data of birth				X			

STANDARD STUDENT DATA PRIVACY AGREEMENT

Version 2.0

Category of Data / Data Elements	Omni Platform	Mindtap, Mindtap School	CNOWv2, OWLv2, Webassign	Ed2go	CIMA	Spark	PRODUCT NAME(S)
Demographics con't							
Place of birth							
Gender							
Ethnicity or race							
Language information (native, or primary language spoken by student)							
Other demographic information							
If 'Other' checked, please specify below checked box:							
Enrollment							
Student school enrollment		MTS, MT	CNOW, OWL, WA		X		
Student grade level							
Homeroom							
Guidance counselor							
Specific curriculum programs							
Year of graduation							
Other enrollment information							
If 'Other' checked, please specify below checked box:							
Parent/Guardian Contact Information							
Address							
Email	X						
Phone							
Parent/Guardian ID							
Parent ID number (created to link parents to students)							
Parent/Guardian Name							
First and/or last							

STANDARD STUDENT DATA PRIVACY AGREEMENT

Version 2.0

Category of Data / Data Elements	Omni Platform	Mindtap, Mindtap School	CNOWv2, OWLv2, Webassign	Ed2go	CIMA	Spark	PRODUCT NAME(S)
Schedule							
Student scheduled courses		MT	CNOW, OWL, WA	X	X		
Teacher names		MT	CNOW, OWL, WA		X		
Special Indicator							
English language learner information							
Low-income status							
Medical alerts/health data							
Student disability information							
Specialized education Services (IEP or 504)							
Living situations (homeless/foster care)							
Other indicator information							
Student Contact Information							
Address				X			
Email		MT	CNOW, OWL, WA	X	X	X	
Phone				X			
Student Identifiers							
Local (School district) ID number		MTS	WA				
State ID number							
Provider/App assigned student ID number			CNOW, OWL, WA		X		
Student App username		MTS, MT	CNOW, OWL, WA	X	X	X	
Student app passwords		MTS		X	X	X	
Student Name							
First and/or last		MTS, MT	CNOW, OWL, WA	X	X	X	

STANDARD STUDENT DATA PRIVACY AGREEMENT

Version 2.0

Category of Data / Data Elements	Omni Platform	Mindtap, Mindtap School	CNOWv2, OWLv2, Webassign	Ed2go	CIMA	Spark	PRODUCT NAME(S)
Student In App Performance							
Program/application performance (e.g. typing program – student types 60 wpm, reading program – student reads below grade level)						X	
Student Program Membership							
Academic or extracurricular activities a student may belong to or participate in							
Student Survey Responses							
Student responses to surveys or questionnaires		MT		X	X		
Student Work							
Student generated content; writing, pictures, etc.		MT	CNOW, OWL, WA	X	X	X	
Other student work data			CNOW, OWL				
If 'Other' checked, please specify below checked box:			File attachments				
Transcript							
Student course grades		MT	OWL, WA	X	X	X	
Student course data		MT	OWL, WA	X	X	X	
Student course grades/performance scores		MT	OWL, WA		X	X	
Other transcript data							
Transportation							
Student bus assignment							
Student pick up and/or drop off location							
Student bus card ID number							
Other transportation data – please specify							
Other							
Please list each additional data element used, stored, or collected by your application:							
None							

No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable							
--	--	--	--	--	--	--	--

If Student Data is stored outside the United States, Provider shall list below the Countries where data is stored:

EXHIBIT C: DEFINITIONS

Change of Control: Any merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of Provider or of the portion of Provider that performs the Services in the Service Agreement.

Contextual Advertising: Contextual advertising is the delivery of advertisements based upon a current visit to a Web page or a single search query, without the collection and retention of data about the consumer's online activities over time.

De-Identified Data: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific student, including, but not limited to, any information that, alone or in combination is linkable to a specific student.

Data Breach: An unauthorized release, access to, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider in violation of applicable state or federal law.

Educational Records: Educational Records shall have the meaning set forth under FERPA 20 U.S. C. 12 32 g(a)(5)(A). For additional context see also the 'Student Data' definition.

LEA: For the purpose of this DPA, the LEA is the educational entity that is a Party to this Agreement. An LEA can be a state agency, an educational service agency, a charter school or school system or a private school or school system, in addition to the federal definition of Local Education Agency (LEA).

Metadata: Means information that provides meaning and context to other data being collected including, but not limited to date and time records and purpose of creation. Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information or Student Data.

Originating LEA: An educational entity otherwise meeting the definition of LEA that originally executes the DPA in its entirety with the Provider.

School Official: For the purposes of this DPA and pursuant to FERPA 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Educational Records; and (3) Is subject to FERPA 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Educational Records.

Service Agreement: Refers to the quote, corresponding contract, purchase order or terms of service and/or terms of use.

Student Data: Student Data includes any data, whether gathered, created or inferred by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose, that is descriptive of the student including, but not limited to, information in the student's Educational Record, persistent unique identifiers, or any other information or identification number that would provide information about a specific student. Student Data includes Metadata that has not been stripped of all direct and indirect identifiers. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed

to be collected or processed by the Provider pursuant to the Services. Student Data shall not include properly De- Identified Data or anonymous usage data regarding a student's or LEA's use of Provider's Services.

Student Generated Content: The term "Student Generated Content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content. "Student Generated Content" does not include student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to or storage of Student Data, including security, storage, analytics, and other processing activities necessary to perform a Provider business purpose.

Subprocessor Agreement: An agreement between Provider and a third party Subprocessor. A Subprocessor Agreement includes either a written agreement or an acceptance of terms and conditions (e.g., click through agreements).

Subscribing LEA: An educational entity otherwise meeting the definition of LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms by executing Exhibit "E".

Targeted Advertising: Targeted Advertising means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the Provider Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include Contextual Advertising.

EXHIBIT D: SPECIAL INSTRUCTIONS FOR DISPOSITION OF DATA

After this DPA takes effect, if the LEA has special requirements for the disposition of Student Data that are not expressed in 4.6 Disposition of Data, the LEA may fill in this form and deliver it to the Provider.

The Provider and the LEA must not fill in this form at the initiation of the DPA.

The Provider shall act on Exhibit “D” from the designated representative of the LEA or their designee (Preamble or Exhibit “E” for Subscribing LEA).

[Insert Name of District or LEA] (“LEA”) instructs Provider to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

☐ Disposition is partial. The scope of Student Data to be disposed of is set forth below or found in an attachment to this Directive:

[Insert categories of Student Data here]

☐ Disposition is complete. Disposition extends to all Student Data.

2. Nature of Disposition

☐ Disposition shall be by destruction or deletion of Student Data.

☐ Disposition shall be by a transfer of Student Data. The Student Data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Timing of Disposition

Student Data shall be disposed of by the following date:

☐ As soon as commercially practicable

☐ On Provider’s standard destruction schedule

☐ By ***[Insert Date]***

4. De-Identified Data

☐ The Provider certifies that they have De-Identified the data, as defined elsewhere in this Agreement, and disposed of all copies of Student Data that were not De-Identified in accordance with this Schedule and the DPA. The Provider will notify LEA in accordance with the notification requirements of the DPA using this form.

As of ***[Insert Date]***

5. Other:

Signature(s)

Notice of Verified Disposition of Data

Authorized Representative of
LEA

Date

Authorized Representative of
Provider

Date

EXHIBIT E: GENERAL OFFERS OF TERMS

Page 1 of 2: OFFER OF TERMS

Provider and the Subscribing LEA (named below) agree by signing this General Offer of Privacy Terms (“General Offer”) that they are bound by the same terms as the DPA between Provider and Fairfax County Public Schools (“**Originating LEA**”) dated 03/05/2025.

Provider and Subscribing LEA agree that the information below will be replaced throughout the DPA with the information specific to the Subscribing LEA filled in below for the Subscribing LEA. This General Offer shall extend only to the terms set forth in this DPA and shall not necessarily bind Provider or Subscribing LEA to any other terms entered into between Provider and Originating LEA. Any commercial terms, such as price, term, or schedule of Services, relating to Subscribing LEA’s use of the Provider’s Services shall be determined solely between Provider and Subscribing LEA.

If Provider makes changes to Exhibit “A” or Exhibit “B” in accordance with sections 1.2 and 1.3 respectively, Provider must complete the Addendum template provided by the A4L Community and notify the Originating LEA and all Subscribing LEAs in accordance with the notification provisions of this DPA, of the Addendum’s existence and contents. With regard to a Subscribing LEA, an Addendum is automatically incorporated into this DPA when Subscribing LEA is notified by Provider. If an Addendum modifies Exhibit “B”, the LEA will have thirty (30) days from receipt to object. If no written objection is received it will become incorporated into the DPA between the parties.

The Provider may withdraw the General Offer (for future use or for LEAs that have not already accepted it) in the event of: (1) a material change in the applicable privacy statutes; or (2) a material change in the Services and products listed in the Service Agreement. Notification of a withdrawal shall be submitted to ndpa_requests@A4L.org.

Subscribing LEAs shall send the signed Exhibit “E” to Provider at the following email address: USK12contractnotices@cengage.com

The below signatory confirms they are authorized to bind their institution to this DPA as in its entirety.

RESOURCE NAME(S):

[Insert all Resource Names covered by Originating DPA]

[]

[]

[]

PROVIDER: Cengage Learning, Inc.

Signed By: Jean D. Yacchari

Date: 03/10/2025

Printed Name: Jean Yacchari

Title/Position: K12 Contracts Program Manager

Exhibit “E” (continued)

Originating LEA:

Resource Names:

Provider Name:

Page 2 of 2: [INSERT NAME] “SUBSCRIBING LEA”

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Originating LEA and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER.**** Please note, by signing this Exhibit you are also agreeing to any language that may be included in Exhibits to the Originating DPA beyond this Exhibit “E”. The below signatory confirms they are authorized to bind their institution to this DPA as in its entirety.

Subscribing LEA: [Insert Name of Subscribing LEA]

Signed By: Michelle Pratt

Date: 4/11/2025 | 1:57 PM EDT

Printed Name: Michelle Pratt

Title/Position: Director, Office of Procurement Svcs

School District Name: Fairfax County School Board

Designated Representative of LEA:

Name:

Title:

Address:

Telephone:

Email:

Notices to Subscribing LEA: The Provider and Subscribing LEA are each responsible to promptly notify the other Party of changes to the notice information.

Security Notices to Subscribing LEA

- [Subscribing LEA Security Name]

[Subscribing LEA Security Role]

[Subscribing LEA Security Postal Address]

[Subscribing LEA Security E-mail Address]
- [Subscribing LEA Name]

[Subscribing LEA Role]

[Subscribing LEA Postal Address]

[Subscribing LEA E-mail Address]
- With a copy to (if provided):
- [Subscribing LEA Legal Counsel]

[Subscribing LEA Legal Counsel Postal Address]

[Subscribing LEA Legal Counsel E-mail Address]

EXHIBIT F: ADEQUATE CYBERSECURITY FRAMEWORKS

Provider must mark one or more frameworks with which it complies.

The Provider may change which framework it complies with without invalidating or changing the DPA, but must notify the LEA of such change in accordance with the notification requirements of the DPA.

FRAMEWORK(S)	
	Global Education Security Standard - https://sdpc.a4l.org/gess/
X	NIST Cybersecurity Framework (CSF)
X	NIST SP 800-53 Security and Privacy Controls for Information systems and organizations
	NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
	ISO 27000 series, Standards for implementing organization security and management practices
	CIS Center for Internet Security Critical Security Controls
	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

This space is provided for optional security programs and measures as noted in section 5.3:

EXHIBIT G: Supplemental SDPC State Terms for [Virginia]

LEA and Provider agree to the following additional or replacement terms and modifications:

Division Data as referenced in Exhibit G includes all business, employment, operational and Personally Identifiable Information that LEA provides to Provider and that is not intentionally made generally available by the Division on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and student, employees, and personnel data, user generated content and metadata but specifically excludes Provider Data (as defined below).

For purposes of this agreement, Student Data as defined in the DPA shall include any employee records and/or employee information that LEA provides to Provider, and the following definition of Student Data in the DPA shall be replaced with the following:

If applicable, student Data includes any data, whether gathered, created or inferred by Provider or provided by LEA or its users, **employees**, students, or students' parents/guardians, for a school purpose, that is descriptive of the student **and/or employee** including, but not limited to, information in the student's Educational Record **and/or the employee's personnel record**, persistent unique identifiers, or any other information or identification number that would provide information about a specific student **and/or employee**. Student Data includes Metadata that has not been stripped of all direct and indirect identifiers. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not include properly De-Identified Data or anonymous usage data regarding a student's **or employee's** or LEA's use of Provider's Services.

In the event that Provider uses Artificial Intelligence in its platform and as a part of its services to Division, then any additional and/or third party terms and conditions shall not be applicable unless separately negotiated and added on as an Amendment to this Agreement.

Provider must comply with all applicable provisions of Virginia law and the Code of Virginia including but not limited to the following:

1. The requirements and operative definitions found in Code of Virginia § 22.1-289.01.
2. Virginia utilizes the FERPA definition of Personally Identifiable Information (PII).
3. Notification of Data Breach: In order to ensure the LEA's ability to comply with its reporting requirements under Virginia Code §2.2-5514(C), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within 72 clock hours, where the service provider confirms Division Data may have been disclosed in a data breach. In addition to this initial notification, Provider shall comply with all relevant requirements and deadlines outlined in this DPA, Article V, Section 4: Data Breach.

9.11. This section must include all proposed terms and conditions including sample contracts and Service Level Agreements (SLA) describing service and support for the system and maintenance and support agreements.



CENGAGE SERVICE LEVEL AGREEMENT

Cengage uses reasonable commercial efforts to ensure that the Digital Products adopted are available no less than 99.5%, exclusive of scheduled maintenance and downtime that is outside of Provider's reasonable control. Most of our updates require no-downtime releases due to our architectural design which allows us to continuously improve without impacting student/faculty availability.

Cengage has multiple layers of support infrastructure to proactively monitor for service issues as well as receive and act upon issues reported by customers. More specifically, we maintain: 270 person, US based contact center that is available for customers during most business hours, 365 days per year 5 person incident and escalation management team that facilitates troubleshooting issues that require involvement from tier 3 development resources. We have market leading logging and diagnostic tools such as Splunk and Dynatrace, as well as real time on-call paging systems, and annually trained issue and communication response processes to address broad impacting issues. All changes to platform and system availability as well as our reports of uptime can be found on our <https://techcheck.cengage.com>

Our services are provided at 99.5% of the time and scheduled maintenance periods most often do not have negative impact on our users, for any service credit, please work with your sales representative.

Cengage Incident Priority, Description and Response Table

Incident Priority	Incident Description	Incident Response Service Level
1	Service is down or unavailable	- Licensor shall provide status updates every 60-90 minutes thereafter unless a difference cadence of updates is mutually agreed upon on a per incident basis. - Licensor will use commercially reasonable efforts to commence efforts to fix such Priority 1 Incident within 1 hour after such notification of such Incident.
2	Service functionality is substantially impacted, or significant Service performance degradation is experienced with high impact to University of Phoenix's business operations	- Licensor shall provide status updates every 4 hours thereafter unless a difference cadence of updates is mutually agreed upon on a per incident basis. - Licensor will use commercially reasonable efforts to commence efforts to fix such incident within 4 hours after such notification of such Incident.
3	There is a partial, non-critical impact to Service functionality or Service performance degradation with low impact to district business operations	- Licensor shall provide status updates every 24 hours thereafter unless a difference cadence of updates is mutually agreed upon on a per incident basis. - Licensor will use commercially reasonable efforts to commence efforts to fix such Priority 3

Incident Priority	Incident Description	Incident Response Service Level
		Incident within 72 hours after such notification of such Incident.
4	- Request for a new service; or - Requests involving routine technical issues; or - Inquiries regarding Service capabilities; or - Notice of minor Service performance issues for which a fix or work around is available	Licensors will respond and/or resolve as soon as possible or within a timeframe as mutually agreed upon on a per incident or request basis.

SECURITY POLICY AND GUIDELINES

Cengage has developed and documented a formal information security policy & guidelines set, which 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 documentation 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 online

9.12. Offerors may take exceptions to the terms, however, some of the terms may not be negotiable. The following contract terms of Appendix A are required by law and cannot be varied, revised, amended, changed or otherwise negotiated: para. 34 (Funding), para. 37 (Non-Discrimination), para. 61 (Authorization to Conduct Business in the Commonwealth), para. 58.d (No Indemnification by the County), para. 68 (Contractual Disputes), para. 72 (Drug Free Workplace), para. 73 (Immigration Reform and Control Act) and para. 74 (Audit of Records).

Exceptions to the Terms & Conditions are in *Attachment E*.

9.13. The personnel named in the technical proposal will remain assigned to the project throughout the period of this contract. No diversion or replacement may be made without submission of a resume of the proposed replacement with final approval being granted by the County Purchasing Agent.

National Geographic Learning/Cengage strives to provide consistency throughout each adoption. All named personnel will most likely remain involved with this contract for its duration as long as there are no unforeseen staff changes.