

STANDARD STUDENT DATA PRIVACY AGREEMENT

TX-NDPA v1r6

School District or LEA

Cypress-Fairbanks ISD

and

Provider

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:

[**Cypress-Fairbanks ISD**], located at [10300 Jones Road Houston, Texas 77065] (the “**Local Education Agency**” or “**LEA**”) and

[], located at [] (the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

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 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

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:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - ☒ If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - ☒ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit “H”**. (Optional)
 - ☐ If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three (3) years. **Exhibit “E”** will expire three (3) years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Charles Franklin Title: Assistant Superintendent of Technology & Information Services

Address: 10300 Jones Road Houston, Texas 77065

Phone: 281.897.4000 Email: dpa@cfisd.net

The designated representative for the Provider for this DPA is:

Name: Pamela LeBlanc Title: Contract Administrator

Address: 27555 Executive Dr., Suite 270 Farmington Hills, MI 48331

Phone: 800-877-4253 X18465 Email: Pamela.LeBlanc@Cengage.com

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

LEA:

By: 
Charles Franklin (Jul 14, 2025 22:00 CDT)

Date: Jul 14, 2025

Printed Name: Charles Franklin Title/Position: Assist. Superintendent of Technology & Information Services

Provider:

By: 

Date: Jul 14, 2025

Printed Name: Brian Risse Title/Position: VP, Gale/Thorndike School Sales

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

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, state, and local 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. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit “C”**. 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, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service 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 transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are 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. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) 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 or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact 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, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements 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 no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
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. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents 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 or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of 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 other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development 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 Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.
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. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data**" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. 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 LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security**. The Provider agrees to utilize 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. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

- iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as 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 breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **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. 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, **Exhibit “H”** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service 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. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **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.
6. **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.
7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. 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. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority**. Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver.** No delay or omission by either party to exercise any right hereunder 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.

EXHIBIT "A"
DESCRIPTION OF SERVICES

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	<input checked="" type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	<input checked="" type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application:	<input checked="" type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

EXHIBIT “C”**DEFINITIONS**

De-Identified Data and De-Identification: 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 individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

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.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

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.

School Official: For the purposes of this DPA and pursuant to 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 Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. 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 constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

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 Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

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 operator's 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 any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"**DIRECTIVE FOR DISPOSITION OF DATA**

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

☐ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

☐ []

☐ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

☐ Disposition shall be by destruction or deletion of data.

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

☐ []

3. Schedule of Disposition

Data shall be disposed of by the following date:

☐ As soon as commercially practicable.

☐ By []

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT "E"**GENERAL OFFER OF PRIVACY TERMS****1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and [Cypress-Fairbanks ISD] ("Originating LEA") which is dated [], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: Pamela.LeBlanc@Cengage.com

[NAME OF PROVIDER]

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

2. 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 [] and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

Subscribing LEA:

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____ Title: _____

Address: _____

Telephone Number: _____ Email: _____

EXHIBIT “F”**DATA SECURITY REQUIREMENTS****Adequate Cybersecurity Frameworks****2/24/2020**

The Education Security and Privacy Exchange (“Edspex”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* (“Cybersecurity Frameworks”) that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input checked="" type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
<input checked="" type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT “G”**Supplemental SDPC State Terms for Texas**
Version 1.0

This **Exhibit “G”**, Supplemental SDPC State Terms for Texas (“Supplemental State Terms”), effective simultaneously with the attached Student Data Privacy Agreement (“DPA”) by and between [Cypress-Fairbanks ISD] (the “Local Education Agency” or “LEA”) and [] (the “Provider”), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Covered Data.** All instances of "Student Data" should be replaced with "LEA Data". The protections provided within this DPA extend to all data provided to or collected by the Provider.
2. **Compliance with Texas Privacy Laws and Regulations.** In performing their respective obligations under the Agreement, the LEA and the Provider shall comply with all Texas laws and regulations pertaining to LEA data privacy and confidentiality, including but not limited to the Texas Education Code Chapter 32, and Texas Government Code Chapter 560.
3. **Modification to Article III, Section 2 of the DPA.** Article III, Section 2 of the DPA (Annual Notification of Rights.) is amended as follows:

~~**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.~~

Consider Provider as School Official. The Parties agree that Provider is a “school official” under FERPA and has a legitimate educational interest in personally identifiable information from education records received from the LEA pursuant to the DPA. For purposes of the Service Agreement and this DPA, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from the education records received from the LEA.

4. **Modification to Article V, Section 4 of the DPA.** Article V, Section 4 of the DPA (Data Breach.) is amended with the following additions: (6) For purposes of defining an unauthorized disclosure or security breach, this definition specifically includes meanings assigned by Texas law, including applicable provisions in the Texas Education Code and Texas Business and Commerce Code. (7) The LEA may immediately terminate the Service Agreement if the LEA determines the Provider has breached a material term of this DPA. (8) The Provider’s obligations shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

5. **Modification to Article VII, Section 4 of the DPA.** Article VI, Section 4 of the DPA (Annual Notification of Rights.) is amended as follows:

Entire Agreement. This DPA ~~and the Service Agreement~~ constitutes 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. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

6. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with:
- a. Providing notification to the employees or parents of those students whose LEA Data was compromised and regulatory agencies or other entities as required by law or contract;
 - b. Providing credit monitoring to those employees or students whose LEA Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the employee's or student's credit or financial security;
 - c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and
 - d. Providing any other notifications or fulfilling any other requirements adopted by the Texas State Board of Education, Texas Education Agency, or under other State or federal laws.
7. **No Exhibit E without unaltered DPA including Texas Addendum.** Any alterations are only allowed in **Exhibit "H"**. Any terms under **Exhibit "H"** do not apply to **Exhibit "E"** and render **Exhibit "E"** null and void.

Exhibit H

Cengage Learning, Inc. and Cypress-Fairbanks ISD

For convenience, language that has been added in the below section is shown in *italics*, and language that has been deleted is shown in strikethrough.

1. Article III.1, *Provide Data in Compliance with Applicable Laws*, is replaced in its entirety with the following text: “LEA shall provide, *and allow Provider to collect*, Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local 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 individual signing this DPA on behalf of the LEA has the authority to authorize the collection of personal information on behalf of the LEA. The Provider’s privacy notices are available at <https://www.cengagegroup.com/privacy/>.*” Attached as Schedule 1
2. Article IV.2, *Authorized Use*, is replaced in its entirety with the following text: “The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit A** or stated in the Service Agreement, *as required to comply with applicable law*, and/or otherwise authorized under the statutes referred to herein this DPA.”
3. Article IV.5, *De-Identified Data*, the second-to-last sentence, is amended by deleting the strikethrough text as follows: “Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless ~~(a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer.~~”
4. Article IV.6, *Disposition of Data*, is amended by deleting the strikethrough text and adding the italicized text as follows: “Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data *according to Provider’s data retention policy after providing the LEA with reasonable prior notice*. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II.3. The LEA may employ a **Directive for Disposition of Data** form, a copy of which is attached hereto as **Exhibit D**. If the LEA and Provider employ **Exhibit D**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit D**. *Notwithstanding the foregoing, Provider may retain Student Data for the purposes of complying with law, provided that the terms of this DPA shall survive and apply with respect to such retained Student Data and Provider shall only use and disclose the retained Student Data for the purposes that require its retention.*”

5. Article V.4(3), *Data Breach*, is amended by deleting the strikethrough text and adding the italicized text as follows: "Provider further acknowledges and agrees to have a written incident response plan that reflects ~~best practices~~ and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon *written* request, with a summary of said written incident response plan."
6. Article VII.1, *Termination*, is replaced in its entirety with the following text: "*In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either Party may terminate this DPA and any Services Agreement or contract while in effect 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.*"
7. Article VII.10, Limitation of Liability, is added as follows: *NOTWITHSTANDING ANYTHING IN THE AGREEMENT OR THE DPA TO THE CONTRARY, AND EXCEPT FOR GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, PROVIDER'S LIABILITY SHALL NOT EXCEED TWO TIMES THE FEES PAID BY THE LEA IN CONNECTION WITH THE PROVISION OF THE SERVICES UNDER THE AGREEMENT DURING THE TWELVE (12) MONTHS PRECEDING THE EVENT GIVING RISE TO THE LIABILITY. IN NO EVENT SHALL PROVIDER BE LIABLE TO THE LEA IN ANY RESPECT, FOR INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL OR PUNITIVE DAMAGES, ARISING OUT OF THE AGREEMENT OR THIS ADDENDUM OR THE ACTS OR OMISSIONS IN FULFILLING ITS OBLIGATIONS HEREUNDER.*
8. Exhibit G, Section 1, *Covered Data*, is amended by adding the italicized text: "All instances of "Student Data" should be replaced with "LEA Data". The protections provided within this DPA extend to all *personal* data provided to or collected by the Provider."
9. Exhibit G, Section 2, *Compliance with Texas Privacy Laws and Regulations*, is amended by adding "applicable" before "Texas laws."

10. Exhibit G, Section 4, *Modification to Article V, Section 4 of the DPA*, is amended by deleting the strike-through text: "(6) For purposes of defining an unauthorized disclosure or security breach, this definition specifically includes meanings assigned by Texas law, including applicable provisions in the Texas Education Code and Texas Business and Commerce Code. (7) ~~The LEA may immediately terminate the Service Agreement if the LEA determines the Provider has breached a material term of this DPA.~~"

Schedule 1 follows on pages 27-45



Cengage Group Privacy Notice Read our Privacy Notice Below:

[PDF Version of the Privacy Notice \(Effective as of June 1, 2025\)](#)

Effective Date: June 1, 2025

What Does this Privacy Notice Cover?

Cengage Learning, Inc. and its subsidiaries (collectively, “Cengage,” “we” and “us”) are a global edtech company comprised of the following brands: Cengage, National Geographic Learning, ed2go, Infosec, Gale, Milady, Nelson, and Visible Body.

This Privacy Notice describes how we collect, use and share personal information from educational professionals (such as teachers, instructors, school administrators, authors, editors and contributors), students at post-secondary schools, adult learners, Ready2Hire participants, website visitors, app users and others with whom we interact. This Privacy Notice also explains how to contact us regarding our privacy practices and the rights and choices you may have related to your personal information.

For information about how we protect the privacy of children and K-12 students, please read our [Privacy Statement regarding K-12 Students' and Children's Data](#). If you have applied for employment with Cengage, please read our [Applicant Privacy Notice](#) for information about our privacy practices with respect to personal information collected as part of the application, interview and recruitment processes. Please also see our additional privacy notices for individuals located outside the United States, available [here](#).

We recommend that you read this entire Privacy Notice so that you are informed about our privacy practices. However, if you want to skip to a particular section in the Privacy Notice, please refer to the table of contents below.

[1. Collection of Your Personal Information](#)

[2. Use of Your Personal Information](#)

[3. Sharing Your Personal Information](#)

[4. Cookies and Other Data Collection Technologies](#)

[5. Forums and Other Public Areas](#)

[6. Tell-A-Friend Functions](#)

[7. Retention of Data](#)

[8. International Transfers](#)

[9. Information Security](#)

[10. Privacy Policies of Third Parties](#)

[11. Your Choices and Rights](#)

[12. Additional U.S. State Privacy Rights](#)

[13. Exercising Your Privacy Rights](#)

[14. Changes to this Privacy Notice](#)

[15. How to Contact Us](#)

1. Collection of Your Personal Information

We collect personal information to deliver the products and services you request, improve our products and services, market to you, host events and support our business functions.

Personal Information We Collect

We collect the categories and types of personal information described below. The categories and types of personal information collected vary depending on your relationship with us.

If you interact with our websites or apps or contact us, we collect the following categories of personal information:

- **Identifiers** that allow us to identify you and communicate with you, such as contact information that you provide us, including your name, mailing address, telephone numbers, email address or other addresses.
- **Internet Network and Device Information** that we collect about your session and your activity and actions when you use our websites and apps or open emails that we have sent you. In addition to any

information that you submit during these sessions, we use cookies and other data collection tools to automatically collect information about your device and your use of our websites and apps, including information about whether and for how long you view videos on our websites and apps. The information we collect includes IP address; internet provider, operating system and browser used; domain names of the computers you use to visit our websites; viewed webpages; links that are clicked; the keystrokes typed; movement of the mouse or pointer; type of device (such as laptop or smart phone); device and advertising identifiers; log files; URIs (Uniform Resource Identifiers) of the resources requested; the time of the request; the method used to submit the request to the server; the size of the file obtained in reply; the numerical status code of the server reply (successful, error, etc.); emails we send that you open, forward or click through to our websites; and other parameters concerning your operating system and computer environment and/or device cookie settings and other device details, such as MAC address. Please see “Cookies and Other Data Collection Technologies” below for additional information.

- **Communication Information** such as the content of emails, text messages, chats or other communications, call logs and chat logs. Additionally, if you participate in a community or forum on our websites or apps, information you share within that community or forum may include personal information.
- **Audio Visual Information** that we collect when you contact us for support. When you contact us, your phone conversation with our support team may be monitored and recorded for training and quality assurance.

If you register for an account with us or purchase or use our products and services, we collect the categories and types of personal information described below, in addition to those categories of personal information described directly above. Note that in some cases we provide our products and services as a “processor” or “service provider” to your educational institution or employer, in which case we process personal information according to instructions from your educational institution or employer and our contract with them. In those instances, the information in this Privacy Notice is intended to provide transparency in relation to our privacy practices and you should refer to the privacy notices of your educational institution or employer to learn more about their privacy practices.

- **Identifiers** that allow us to identify you, such as your name, the account number or user id that we assign you, username and password, email address, IP address, and similar identifiers.
- **Internet Network and Device Information** about how you interact with Cengage, including your download history, activity and actions

within our products and information about your use of our content (including time spent on material and results of in-product assessments).

- **Customer Records**, which include personal information we collect to help us do business and interact with you, such as customer account information. It also includes personal information we require to fill your accessibility requests, such as personal information about your accessibility needs and materials and products that you use for accessibility. We may also collect the following personal information, depending on the product:
 - *If you are a student:* We may collect information about your education, school affiliation, expected degree and graduation date, your courses of study, grades, learning style, languages spoken, age range, responses to quizzes and course work, badges earned, files or content you upload and in some products, messages you send to instructors or the comments you post in a discussion forum.
 - *If you are an instructor:* This may include information about your school affiliation, professional credentials, courses you teach, teaching style, grading and assessments, files or content you upload and in some products, messages you send to students or the comments you post in a discussion forum.
 - *If you are an adult learner:* This may include your employer, job title, professional credentials and affiliations, language spoken, age range, courses of study, time spent in the course (including time and day of course access), overall score in course, completion date and in some products, messages you send to your instructors or the comments you post in a discussion forum.
- **Commercial Information** about your purchase and transaction history with us. We also collect payment card information as needed to process your payment when you purchase products.
- **Geolocation Data**, which includes information about your location if the product you are using uses an identity management service.
- **Audio Visual Information**, such as photographs and video and audio recordings that are captured when you participate in a course.

For ed2Go or Infosec products, we also collect the categories and types of personal information described below:

- **Protected Class Information**, such as military status.
- **Identifiers**, such as date of birth associated with your account information. In some cases, we also collect income information and employment-related outcomes data. When Infosec IQ customers

provision users from their Google workspace directory, we may also collect Google Workspace directory data (“Google Data”) associated with users and groups.

- **Commercial Information** about your purchase and transaction history in relation to the Ed2go course, including information about financing or government funding you receive or your library card number (if you are registering for the course through your public library).

For Clinical Experience (Externship) thru ed2Go, we also collect the categories and types of personal information described below:

- **Educational Information**, such as your education history and course grades.
- **Professional Information**, such as your work history, certifications/licenses and resume/cover letter.
- **Customer Records**, which include personal information we collect to help us do business and interact with you such as background check results (pass/fail), drug screening results (pass/fail) (if required by externship providers) and information related to logistics about the opportunity (e.g., transportation to opportunity).
- **Sensitive Personal Information** includes driver’s license/state identification card, passport and limited vaccination information (if required for the externship).

In connection with Ready2Hire, in addition to those categories of personal information described above under “Personal Information We Collect- If you interact with our websites or apps or contact us,” we collect the categories and types of personal information described below:

- **Protected Class Information**, such as eligibility to work in the United States.
- **Education Information**, such as your education history and course grades.
- **Professional Information**, such as your work history, certifications/licenses and resume/cover letter.
- **Customer Records**, which include personal information we collect to help us do business and interact with you such as background check results (pass/fail), drug screening results (pass/fail) (if required by Ready2Hire partners) and information that you provide us as part of the screening interview and application process (e.g., information related to logistics about the opportunity such as access to internet and transportation to opportunity).
- **Sensitive Personal Information** includes information on whether you received a COVID-19 vaccine (if required by the Ready2Hire partner).

In connection with Gale Business Directories, we collect the categories and types of personal information described below:

- **Identifiers** such as publicly available business contact information about corporate executives, academics and professionals.

Gale, a Cengage company, publishes business directories, which contain publicly available business contact information about corporate executives, academics and professionals obtained from third-party sources. These directories do not contain any information collected from users of Cengage's other products, websites or apps. These directories are used by students, researchers and other professionals to identify relevant corporate contacts, experts and sources. We respect the rights of individuals to opt-out of having their business contact information included in these directories. If you would like to remove your information from our professional directories, please [complete this form](#).

If you participate in research, surveys, feedback or advisory councils (together, "Research") related to Cengage or its products, we collect the categories and types of personal information described below:

- **Identifiers** that allow us to identify you and communicate with you, such as your name, mailing address, telephone numbers, email address, other addresses and electronic signature.
- **Customer Records**, which include personal information we collect to help us do business and interact with you, such as your school affiliation, role at a school (e.g., student, instructor, teacher, administrator), area of study, geographic location, age, years of experience, your use of Cengage products and feedback you provide in relation to Research.
- **Audio Visual Information**, such as photographs and video and audio recordings that are captured, recorded or provided when you participate in Research.
- **Financial Information** that allows us to pay you if there is a payment in connection with your participation in Research, such as your tax identification number, date of birth and bank account information.
- **Communication Information** such as the content of emails, text messages, chats or other communications, call logs and chat logs.
- **Sensitive Personal Information** includes personal information that you provide us if you participate in a survey or provide us feedback related to accessibility, such as personal information about your condition, assistive technology you use and your level of proficiency.

If you participate in a Cengage event (virtual or in-person), we collect the categories and types of personal information described below:

- **Identifiers** that allow us to identify you and communicate with you, such as your name, mailing address, telephone numbers, email address and other addresses.
- **Customer Records**, which include personal information we collect that to help us do business and interact with you, such as your affiliation with an educational institution or corporation, position at an educational institution or corporation, information about your use of Cengage products or content and feedback you provide in relation to an event.
- **Commercial Information** includes personal information we collect in relation to your registration and attendance at a Cengage event, including payment information, information about your travel and lodging, dietary restrictions, visa/passport information (if required in connection with your attendance) and accessibility information that you provide us.
- **Audio Visual Information**, such as photographs and video and audio recordings that are captured, recorded or provided in connection with an event.
- **Communication Information** such as the content of emails, text messages, chats or other communications, call logs and chat logs.

Sources of Personal Information

We collect and receive personal information in a variety of ways: (i) directly from you, (ii) automatically when you take certain actions, and (iii) from third parties.

Directly From You. Except as described in this “Sources of Personal Information” section, we generally collect the personal information described above under “Personal Information We Collect” or any other information you choose to provide directly from you. For example, you share personal information when you create an account with us, purchase or use our products, register with us, sign up to receive materials electronically, request customer service, contact us, participate in an event with us, participate in a promotion or survey, use certain features on our websites and mobile services, or interact with us for any other purpose.

Automatically When You Take Certain Actions. When you access our websites and apps or use our products, we (and other entities) automatically collect the device and usage information set out under “Internet Network and Device Information” above. For more information about the use of this information and choices that may be available to you, please see “Cookies and Other Data Collection Technologies” below.

From Third Parties. We also collect personal information from third parties. Here are some examples of categories of personal information collected from third parties:

- **Identifiers:** Your educational institution or employer may provide us Identifiers about you if they purchase Cengage products for your use. We also receive Identifiers from learning management systems (LMS) and third-party products and services that integrate with or complement our products. Additionally, if you interact with us through a social media service or log in using social media credentials, depending on your social media settings, we may have access to Identifiers from that social network such as your name, email address, age, gender and location. We also may receive Identifiers about prospective customers from third-party lead providers.
- **Business Contact Information for Gale Directory Products:** We obtain publicly available business contact information about corporate executives, academics and professionals for Gale Directory products from third-party sources, such as company websites, publications, public record providers and other commercial sources. These directories do not contain any information collected from users of our products, websites or apps.
- **Customer Records:** We receive personal information from your educational institution, such as information about the classes you are teaching or taking, and from third-party data suppliers who enhance our files and help us better understand our customers. We also receive Customer Records, such as background check confirmations, from our service providers in connection with Externship thru ed2Go. If you register for an Ed2go course through one of our educational partners or through a library, we receive information about you from the educational partner or the library.
- **Commercial Information:** We receive Commercial Information from service providers, such as fraud checks or flags raised about transactions, payment card refusals, suspected crimes, complaints and/or claims. If you register for an Ed2go course through one of our educational partners or through a library, we receive information about your payment, funding and transaction history.

2. Use of Your Personal Information

Depending on your relationship with us, we use your personal information for the following purposes:

- To provide you with the products, content or services selected by you (or your education institution or employer) and for related activities, such as customer service, account management, support,

accessibility accommodations, training, reporting and other services related to your or your educational institution's or employer's account.

- To provide and improve product functionality, such as when we use Google Data to provision Infosec IQ users in customer accounts.
- To communicate with you (including through ads on social media platforms), to provide you with additional information that may be of interest to you and to manage your communications preferences.
- To help ensure the security and integrity of our websites, apps, products, services, systems, networks and facilities (including physical security, cybersecurity, fraud detection and prevention and intellectual property protection), and to undertake activities to verify, maintain and improve the quality and safety of our websites, apps, products, services, systems, networks and facilities.
- To provide advertising and marketing, including sending marketing communications and offers for products and services from Cengage and our partners as well as personalized offers and targeted advertising.
- To administer surveys, sweepstakes and other promotional events.
- To determine if you are eligible for certain products, services or offers, such as rebates or content guides, offered for certain courses.
- To understand how you use our products, content and services (including associating you with the different devices you may use to access our content), for analytics, for research and development, to create new products and services and improve existing products and services, to understand the impact of industry developments and to improve your user experience.
- To host and manage events.
- To manage our everyday business needs, such as payment processing and financial account management, contract management, website administration (including to optimize our websites and apps and for information security purposes), business continuity and disaster recovery, security and fraud prevention, risk management, corporate governance, training, quality control, reporting and legal compliance.
- For relationship purposes, such as use of photos and videos for social media purposes.
- To conduct auditing and monitoring of transactions and engagement, including related to counting and ad impressions to unique visitors, verifying positions and quality of ad impressions, and auditing compliance.
- Short-term transient use, such as non-personalized advertising shown as part of your current interaction with us.
- With your consent, or as otherwise disclosed at the time information is collected.

We may use information that has been deidentified or aggregated without limitation.

3. Sharing Your Personal Information

We share your personal information, to the extent permitted by applicable law, as follows:

- **Within the Cengage group of companies.**
- **If you are affiliated with an educational institution, with your school and if you are a student, with your instructors.** For example, we provide our institutional clients with reports about how their instructors and students use our products, including information that compares instructors and students within a school. If you are a student, your instructors will have access to the information generated by your use of a product for a class and certain information that you enter into the product. We may also provide personal information to your school, as needed, to investigate possible academic fraud or cheating. Your school uses your personal information in accordance with its own privacy policies.
- **If you are affiliated with a corporation who has obtained our products, with your employer.** If your employer has obtained our products for its employees' use and we are processing personal information as a "processor" or "service provider," we may provide your employer with reports about how its employees use the product. Your employer may also have access to the information generated by its employees' use of the product and information that its employees have entered into the product. Your employer uses your personal information in accordance with its own privacy policies.
- **With our service providers and advisors** to the extent necessary to perform services for us or on our behalf. We share Google Data with Google only as needed to provide and improve the provisioning of Infosec IQ users as configured by our customers.
- **With learning management systems (LMS) and other education software providers** that may integrate with or complement our products. These providers are given limited access to personal information in order to deliver the service.
- **Advertisers** who perform advertising and marketing services on our behalf. We may also permit these third parties to collect information directly from you on our websites and apps.
- **With authorized partners that provide services to you** through My Cengage, MindTap and similar platforms but only to the extent that you have authorized the sharing. For example, you may request that Cengage share information about the courses you've taken with partners to enable the partner to provide you with resume creation,

skills assessments or other services. Additionally, we may share certain transactional information with our partners as needed to validate referrals and operate the platforms.

- **With companies** where you are participating in, or seeking to participate in, a program in connection with Clinical Experience (Externship) through Ed2go or Ready2Hire.
- **With your consent or at your direction.**
- **With other third parties**, as permitted by law, to enforce our rights, including our Terms of Use or Terms of Service; to protect our property or to protect the rights, property or safety of others; and to detect, prevent and respond to fraud, illegal activity and intellectual property infringement.
- **With law enforcement agencies, government agencies, regulators and courts** in the United States and other countries where we operate, such as in response to a subpoena or court order or to fulfill a legal obligation.
- **With third parties in connection with, or as part of the due diligence for, any proposed or actual merger, acquisition, sale or transfer** of some or all our assets (including in the event of a reorganization, dissolution or liquidation).

We may share information that has been deidentified or aggregated without limitation.

For individuals who contact Ed2Go for more information: If you provide your consent to receive text messages from Ed2Go, we do not share your consent with third parties.

4. Cookies and Other Data Collection Technologies

When you visit our websites, use our apps or interact with emails we have sent you, we collect information by automated means, using technologies such as cookies, pixel tags, browser analysis tools, server logs and web beacons. In some cases, we may associate the information collected using cookies and other data collection technologies with other personal information we have collected about you. Please refer to our [Cookies Notice](#) for more information on our use of cookies and other data collection technologies and how you can manage such technologies.

Digital Analytics

We may work with third parties that collect data about your use of our websites and services over time for non-advertising purposes. For example, we use Google Analytics to improve the performance of our websites and for other analytics purposes. For more information about how Google Analytics collects and uses data when you use our websites,

visit www.google.com/policies/privacy/partners, and to opt out of Google Analytics, visit tools.google.com/dlpage/gaoptout.

Additionally, many web browsers have settings allowing users to limit the use of cookies or delete cookies. Please be aware that limiting or deleting cookies may make certain functions of our websites unavailable.

Third-Party Advertising Companies

We have relationships with third-party advertising companies to place advertisements on our websites and other companies' websites, except for our websites that process K-12 Student Data, and to perform tracking and reporting functions for Cengage websites and other websites. These third-party advertising companies may place cookies and other data collection technologies on your computer when you visit our websites or other websites so that they can display targeted advertisements to you.

For more information about third-party advertising, please visit the Network Advertising Initiative (NAI) at www.networkadvertising.org. You can opt-out of targeted advertising by certain third-party advertising companies by visiting www.networkadvertising.org/consumer/opt_out.asp or <https://optout.networkadvertising.org/?c=1>.

To learn more about third-party advertising and how to opt out of this advertising on websites by companies participating in the Digital Advertising Alliance (DAA) self-regulatory program, you may visit the DAA Webchoices tool at www.aboutads.info. You can also exercise choices regarding interest-based advertising on your mobile device by downloading the appropriate version of the DAA's AppChoices tool at <https://youradchoices.com/appchoices>.

If you are a resident of a state with an applicable state privacy law, please also see "Additional U.S. State Privacy Rights" below for more information related to third-party advertising and opt-out rights.

Third-Party Websites

This Privacy Notice addresses the use and sharing of personal information by Cengage only and does not apply to your use of a third-party site. Other websites that may be accessible through our websites and apps have their own privacy policies and data collection, use and disclosure practices. For example, our MindTap product uses the YouTube API Services. MindTap uses these services to allow instructors to add videos and the information collected and shared includes meta data that is used to describe the content of the videos delivered in the search results.

Our websites and apps may also enable you to interact with us and others via integrated social media tools or “plug-ins.” If you use these tools to share personal information or you otherwise interact with these features, those companies may collect information about you and may use and share information in accordance with your account settings, including by sharing such information with the general public. Your interactions with third-party companies and your use of their features are governed by the privacy policies of the companies that provide those features. We encourage you to read the privacy notices of these companies.

In addition, if you use these platforms, we may collect personal information about you, as permitted by the platform’s privacy policies. For example, we may allow you to sign into Cengage websites and apps using social media, such as Facebook Connect. If you choose to do this, we may collect personal information about you and your connections.

5. Forums and Other Public Areas

Our websites, apps and products may provide forums and other public areas where individuals can communicate. Prior to posting in these areas, please read the Forum Rules and Terms of Service carefully. All the information you post will be viewable to anyone with access to the area, and any personal information you include in your posting may be read, collected and used by others.

6. Tell-A-Friend Functions

We may offer “tell-a-friend” functionality on our websites. If you choose to use this function, we will collect contact information for your friend. We will automatically send your friend a one-time email with the information you specified or inviting them to visit the site. We use this information for the sole purpose of sending this one-time email and do not retain the information.

7. Retention of Data

We will retain your personal information in accordance with our retention policies for as long as is reasonably necessary to accomplish the purpose for which the information was collected or for the period that may be required or permitted by law, such as for business, legal, accounting or reporting requirements. In determining the length of the retention period, we will consider the amount, nature and sensitivity of personal information; the potential risk of harm from unauthorized use or disclosure of personal information; the purposes for which we process personal information and whether we can achieve those purposes through other means; and applicable legal requirements.

8. International Transfers

Your personal information may be transferred to, stored at or processed in the United States and other countries which may not have equivalent privacy or data protection laws as the country where you are located. However, regardless of where your personal information is transferred, we will protect it in accordance with this Privacy Notice and applicable laws.

When required by applicable data protection laws, we use approved Standard Contractual Clauses or other approved data transfer mechanisms to help assure that personal information is adequately protected when it is transferred to countries without an adequate level of data protection. To learn more about our cross-border transfers of personal information, please [Contact Us](#).

9. Information Security

We use physical, technical, organizational and administrative safeguards designed to help protect your personal information against unauthorized or unlawful processing and against damage, accidental loss or destruction.

10. Privacy Policies of Third Parties

This Privacy Notice addresses the use and sharing of personal information by Cengage only and does not apply to your use of a third-party site. Other websites that may be accessible through our websites and apps have their own privacy policies and data collection, use and disclosure practices. We encourage you to familiarize yourself with the privacy notices provided by all third parties prior to providing them with information or taking advantage of an offer or promotion. For example, our MindTap product uses the YouTube API Services. MindTap uses these services to allow instructors to add videos and the information collected and shared includes meta data that is used to describe the content of the videos delivered in the search results.

11. Your Choices and Rights

You have the following choices in relation to your personal information:

- In many cases, you can choose what personal information to provide to us. Our data collection forms indicate when it is required that you provide personal information for a particular product or service. If you choose not to provide personal information that is required, we may not be able to provide the product or service you request or a particular feature of that product or service.
- If you have an online account with Cengage, you can access and update certain of your personal information by logging into your account. You can also update your communications preferences within your account.
- We respect the rights of individuals to opt-out of having their business contact information included in Gale Directory products. If

you would like to remove your information from Gale Directory products, please complete this form.

- You can always opt-out of receiving marketing communications from us by clicking on the opt-out link in the commercial emails we send. You can also have your name removed from our email marketing lists by contacting our Customer Service department by email at: cengagebrain.support@cengage.com or by phone at +1 800.354.9706 (M -F, 8:00 am -6:00 pm ET).

Please note that even if you opt-out of marketing emails, we may still need to contact you with important information about your account, about the products or services you purchased and for other transactional and informational purposes. For example, even if you opt-out of marketing emails, we will still send you activity or billing confirmations.

Depending on where you are located and the data protection laws that apply, you may have certain rights in relation to your personal information.

Please see “*Additional U.S. State Privacy Rights*” below for a description of the rights available to certain U.S. state residents.

Please see “*Exercise Your Rights*” below for information on how to exercise your rights in relation to your personal information.

12. U.S. State Privacy Rights

This section of the Privacy Notice applies to residents of U.S. states with applicable privacy laws.

Additional Information about Our Collection, Use and Disclosure of Personal Information

- We collect (and in the 12-month period prior to the Effective Date of this Privacy Notice have collected) the categories of personal information from the sources indicated as set out above under “Collection of Your Personal Information.”
- We use (and in the 12-month period prior to the Effective Date of this Privacy Notice have used) personal information for the commercial and business purposes described above under “Use of Your Personal Information.” We may use and share deidentified information to the extent permitted by applicable law. When we use deidentified information, we maintain and use the information in deidentified form and do not attempt to reidentify it, except to check whether our deidentification processes satisfy the requirements of applicable law.

- We sell (and in the 12-month period prior to the Effective Date of this Privacy Notice have sold) the following categories of personal information: Identifiers (i.e., publicly available business contact information of corporate executives, academics and professionals) in connection with our Gale Directory products. See “Collection of Your Personal Information” for more information.
- We share (and in the 12-month period prior to the Effective Date of this Privacy Notice have shared) the following categories of personal information with third-party advertisers and social media platforms for the purpose of cross-context behavioral advertising: Identifiers, Internet Network and Device Information and Customer Records.
- We do not have actual knowledge about selling or sharing personal information of consumers under the age of 16.
- We disclose (and in the 12-month period prior to the Effective Date of this Privacy Notice have disclosed) the categories of personal information to the recipients indicated below for the purposes set out above under “Use of Your Personal Information.” In addition to the disclosures in the table below, if the circumstances described under “Sharing Your Personal Information” arise, we may disclose all categories of personal information to other third parties; law enforcement, government agencies, regulators and courts; and to third parties in connection with a corporate transaction.

Category of Recipients	Category of Personal Information
Service Providers and Advisors	Identifiers, Internet Network and Device Information, Communication Information, Audio Visual Information, Customer Records, Commercial Information, Geolocation Data, Financial Information, Protected Class Information, Educational Information, Professional Information, Sensitive Personal Information
Educational Institution or Employer	Identifiers, Internet Network and Device Information, Communications Information, Audio Visual Information, Customer Records
LMS and Education Software Providers	Identifiers, Internet Network and Device Information, Customer Records
Authorized Partners	Identifiers, Customer Records
Clinical Experience/Ready2Hire Partners	Identifiers, Customer Records, Educational Information, Professional Information, Protected Class Information, Sensitive Information
Advertisers	Identifiers, Internet Network and Device Information, Customer Records

We process Sensitive Personal Information only for the purposes permitted under California privacy law.

State Privacy Rights

Depending on your state of residence, you may be able to exercise the following rights regarding personal information, subject to certain exceptions and limitations:

- *Right to Know and Access:* The right confirm whether we process personal information about you and to know what personal information we have collected, used, disclosed and sold about you, including the categories of personal information; the categories of sources from which the personal information is collected; the business or commercial purpose for collecting, selling or sharing personal information; the categories of personal information that we have sold or disclosed for a business purpose; the categories of third parties to whom we have disclosed personal information; and the specific pieces of personal information we have collected about you.
- *Right to Correct:* The right to correct inaccuracies in your personal information, taking into account the nature of the personal information and the purposes of the processing.
- *Right to Portability:* The right to obtain a copy of your personal information in a portable, and to the extent technically feasible, readily usable format that allows your data to be transmitted to another controller where the processing is carried out by automated means.
- *Right to Delete:* The right to request that we delete personal information we have collected about you.
- *Right to Opt-Out:* The right to opt-out of the (i) “sale” of your personal information, as defined by applicable law; (ii) processing and/or sharing of personal information for targeted advertising; and (iii) profiling in furtherance of decisions that produce legal or similarly significant effects.
- *Right to Request List of Third-Party Recipients:* Certain residents have the right to receive a list of third parties (other than our service providers) to which we have disclosed personal information, subject to certain exceptions.
- *Right to Appeal:* Certain residents have the right to appeal our decision if we deny your privacy request.
- Right not to receive discriminatory treatment for the exercise of the above privacy rights.

13. Exercising Your Privacy Rights

There are several ways for you to exercise your privacy rights:

- You can exercise your privacy rights by submitting this form: [Privacy Rights Request Form](#). You may also submit a request by contacting us at 1-855-477-9840.
- You can request to opt-out of the sale or sharing of your personal information in Gale Directory products by submitting this form: [opt-out of sale and sharing form](#).
- You can opt-out of the sale or sharing of your personal information in relation to cookies by following the instructions [here](#). Certain mechanisms may also be used to signal your opt-out preferences to entities that process personal data. To the extent we are able to recognize signals from these universal opt-out mechanisms and they are legally sufficient, we will process these signals as requests to opt out of processing for the purposes of targeted advertising or the sale of personal data. Depending on the opt-out mechanism you select, the opt out may apply only to certain interactions, such as a specific browser or device. You may select and install an opt-out mechanism of your preference per the provider's instructions.

Where Cengage acts as a “processor” or “service provider” to an educational institution or a company, your request to exercise your privacy rights should be directed to your educational institution or employer. In such cases, we cannot fulfill such rights unless directed to do so by your educational institution or employer.

When you exercise your rights and submit a request to us, we will verify your identity and that the rights you are exercising are available under the data protection laws in your jurisdiction. We may verify your identity by asking you to log in to your account if you have one with us or asking you to provide additional information to verify your identity. We may also use a third-party verification provider to verify your identity.

Applicable data protection laws may also allow you to designate an authorized agent to make a request on your behalf. As permitted by applicable law, when we verify your agent's request, we may verify both your and your agent's identities and request that you directly confirm with us that you provided the authorized agent permission to make the request on your behalf. To protect your personal information, we reserve the right to deny a request from an agent that does not submit proof that they have been authorized by you to act on your behalf.

Applicable data protection laws may require or permit us to decline your privacy request. If we decline your request, we will tell you the reason why, unless we are not permitted by law to share the reason. Certain data protection laws may allow you to appeal a decision we have made regarding your request. To appeal a decision, you may contact us by sending us an email with the subject line “Appeal” to privacy@cengage.com.

The fact that you have elected to exercise your privacy rights will not have an adverse effect on the price and quality of our products or services.

14. Changes to this Privacy Notice

From time to time, we may update this Privacy Notice. When we update this Privacy Notice, we will revise the Effective Date located at the top of this Privacy Notice and will post the updated Privacy Notice on our websites and apps. Additionally, if the changes will materially affect the way we use or disclose previously collected personal information, we will notify you about the change by sending a notice to the primary email address associated with your account.

15. How to Contact Us

Please contact the Cengage Privacy Office at privacy@cengage.com if you have any questions or comments about our privacy practices or this Privacy Notice.

If you are reaching out to us about a vulnerability in our websites, apps or products, please email security@cengage.com.









Cengage Learning, Inc._CFISD TX_NDPA_V1_ with_exhibit H_final 6-23-25
















Final Audit Report

2025-07-15

Created:	2025-06-23
By:	Helen Jackson (HELEN.JACKSON@cfisd.net)
Status:	Signed
Transaction ID:	CBJCHBCAABAACJhqR-ix_SIWm69G12eZbIW3WTEHUINz
Number of Documents:	1
Document page count:	45
Number of supporting files:	0
Supporting files page count:	0

"Cengage Learning, Inc._CFISD TX_NDPA_V1_with_exhibit H_fi nal 6-23-25" History

-  Document created by Helen Jackson (HELEN.JACKSON@cfisd.net)
2025-06-23 - 5:40:30 PM GMT
-  Document emailed to Pamela LeBlanc (pamela.leblanc@cengage.com) for approval
2025-06-23 - 5:42:39 PM GMT
-  Email viewed by Pamela LeBlanc (pamela.leblanc@cengage.com)
2025-06-23 - 5:42:50 PM GMT
-  Agreement viewed by Pamela LeBlanc (pamela.leblanc@cengage.com)
2025-06-23 - 5:42:56 PM GMT
-  Document approved by Pamela LeBlanc (pamela.leblanc@cengage.com)
Approval Date: 2025-06-23 - 6:13:59 PM GMT - Time Source: server
-  Document emailed to Brian Risse (brian.risse@cengage.com) for signature
2025-06-23 - 6:14:04 PM GMT
-  Email viewed by Brian Risse (brian.risse@cengage.com)
2025-06-23 - 6:14:09 PM GMT
-  Agreement viewed by Brian Risse (brian.risse@cengage.com)
2025-06-23 - 6:14:12 PM GMT

-  Helen Jackson (HELEN.JACKSON@cfisd.net) added alternate approver toni.mcpherson@cfisd.net. The original approver Jennifer Grimm (Jennifer.Grimm@cfisd.net) can still approve.
2025-06-26 - 8:36:16 PM GMT
-  Email viewed by Brian Risse (brian.risse@cengage.com)
2025-07-14 - 6:48:29 PM GMT
-  Document e-signed by Brian Risse (brian.risse@cengage.com)
Signature Date: 2025-07-15 - 2:30:22 AM GMT - Time Source: server
-  Document emailed to toni.mcpherson@cfisd.net for approval
2025-07-15 - 2:30:28 AM GMT
-  Document emailed to Jennifer Grimm (Jennifer.Grimm@cfisd.net) for approval
2025-07-15 - 2:30:28 AM GMT
-  Document emailed to Charles Franklin (Charles.Franklin@cfisd.net) for signature
2025-07-15 - 2:30:29 AM GMT
-  Email sent to Jennifer Grimm (Jennifer.Grimm@cfisd.net) bounced and could not be delivered
2025-07-15 - 2:30:39 AM GMT
-  Email viewed by Charles Franklin (Charles.Franklin@cfisd.net)
2025-07-15 - 3:00:14 AM GMT
-  Agreement viewed by Charles Franklin (Charles.Franklin@cfisd.net)
2025-07-15 - 3:00:20 AM GMT
-  Document e-signed by Charles Franklin (Charles.Franklin@cfisd.net)
Signature Date: 2025-07-15 - 3:00:39 AM GMT - Time Source: server
-  Email viewed by toni.mcpherson@cfisd.net
2025-07-15 - 11:31:11 AM GMT
-  Agreement viewed by toni.mcpherson@cfisd.net
2025-07-15 - 11:31:37 AM GMT
-  Signer toni.mcpherson@cfisd.net entered name at signing as Toni McPherson
2025-07-15 - 11:32:06 AM GMT
-  Document approved by Toni McPherson (toni.mcpherson@cfisd.net)
Approval Date: 2025-07-15 - 11:32:11 AM GMT - Time Source: server
-  Agreement completed.
2025-07-15 - 11:32:11 AM GMT