

## West Irondequoit Central School District

### Data Privacy Agreement for Vendors / Contractors / Service Providers

This Agreement supplements the underlying Contract to which it is attached to ensure that the underlying Contract conforms to the requirements of New York State Education Law Section §2-d and related Regulations of the Commissioner of Education. To the extent that any term of the Contract conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

As used in this Agreement, protected Data includes all Personally Identifiable Information (PII) as defined in New York Education Law Section §2-d, and other non-public data, including, but not limited to, staff data, student data, metadata, and user content. Examples of protected Data include, but are not limited to, names, e-mail addresses, ID numbers, date of birth, and demographic information.

#### 1. Data Privacy

Service Provider agrees that the security, confidentiality, and integrity of protected Data shall be maintained in accordance with state and federal laws that protect the confidentiality of personally identifiable information, and also in accordance with District's Parents Bill of Rights for Data Security and Privacy, provided below.

#### 2. Data De-Identification

Service Provider may use de-identified Data for product development, research, or similar purposes. De-identified Data must have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, and location information. Furthermore, Service Provider agrees not to attempt to re-identify any de-identified Data, and not to transfer de-identified Data to any party unless that party agrees not to attempt re-identification.

#### 3. Marketing and Advertising

Service Provider will not use any Data to advertise or market to students, their parents, faculty or staff. The exclusive purpose for which Service Provider is being provided access to protected Data is for providing WICSD with the functionality of the Products or Services accessed by the school district. Protected Data received by Service Provider, or by any assignee of Service Provider, from WICSD shall not be sold or used for marketing purposes.

#### 4. Data Sharing

Service Provider agrees that it will disclose protected Data received from WICSD only to those officers, employees, and agents who need access to provide the contracted services. Service Provider further agrees to ensure that subcontractors or other entities to whom the Service Provider discloses protected Data will abide by all applicable Data protection and security requirements, including, but not limited to, those outlined in applicable state and federal laws and regulations.

#### 5. Data Privacy Training

Service Provider ~~endures~~ will require that any of its officers or employees, and any officers or employees of any assignee or subcontractor who have access to personally identifiable information, will receive training on the federal and state laws governing confidentiality of such Data prior to receiving access to that Data.

#### 6. Access and Correction

Service Provider agrees to support access to and correction of Data by the District or, when applicable, by the student or their authorized parent when the Data is collected directly from the student with student/parent consent, consistent with the Family Educational Rights and Privacy Act (FERPA).

## **7. Data Use and Collection**

Service Provider will only collect and use Data necessary to provide WICSD with the functionality of the Products or Services accessed by the school district. Service Provider will disclose, in a manner easy for parents to understand, what types of student personal information is collected and for what purpose.

## **8. Rights and Licenses to Data**

Service Provider has a limited, non-exclusive license solely for the purpose of performing its obligations as outlined in the Terms of Agreement. This Agreement does not give Service Provider any rights, implied or otherwise, to Data, content, or intellectual property, except as expressly stated in the Agreement. This includes the right to sell or trade Data.

## **9. Data Transfer or Destruction**

Service Provider will ensure that all Data in its possession and in the possession of any subcontractors, or agents to which the Service Provider may have transferred Data, are destroyed or transferred to the District upon expiration of this Agreement without a successor contract in place, or upon request from the District.

## **10. Data Protection**

- a. Service Provider will take measures aligned with industry best practices, state and federal regulations such as Ed Law Section 2-d and related Commissioner's Regulations, and the NIST Cybersecurity Framework and reasonably designed to protect the privacy and security of protected data while it is stored and in transit. Such measures include, but are not necessarily limited to, encryption technology, firewalls, and password protection.
- b. Service Provider will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of protected data in its custody.
- c. Service Provider will conduct periodic risk assessments, remediating any identified security vulnerabilities in a timely manner.
- d. Service Provider will maintain a written incident response plan, to include prompt notification of the District in the event of a security or privacy incident, as well as best practices for responding to a breach of protected data.
- e. Service Provider agrees to share its incident response plan upon request.
- f. In the event of a breach or unauthorized release of protected data by the Service Provider or subcontractor, the Service Provider will notify the District of the breach in the most expedient way possible and without unreasonable delay, but not more than 7 calendar days from awareness of incident. The Service Provider and the third party contractor may be subject to penalties as outlined in Education Law §2-d.
- g. Service Provider will ensure by contractual agreements or other legally binding measures that any subcontractor, assignee, or agent (including any Hosting Service Provider) to whom Service Provider discloses protected data will comply with the same data security and privacy standards required of Service Provider under this agreement and applicable state and federal laws.

### **References:**

- <https://studentprivacy.ed.gov/audience/education-technology-vendors>
- <http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/parents-bill-of-rights.pdf>
- [https://www.westirondequoit.org/UserFiles/Servers/Server\\_228510/File/DISTRICT/Parents\\_Bill\\_of\\_Rights.pdf](https://www.westirondequoit.org/UserFiles/Servers/Server_228510/File/DISTRICT/Parents_Bill_of_Rights.pdf)
- <https://www.nysenate.gov/legislation/laws/EDN/2-D>
- <http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/proposed-part-121-for-pii.pdf>

## PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The West Irondequoit Central School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by New York State is available for public review at the following website <http://www.nysed.gov/student-data-privacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure>. Complaints may also be submitted to the District's Data Protection Officer by writing to: Data Protection Officer, West Irondequoit Central School District, 45 Cooper Road, Rochester, NY 14617.

## APPENDIX

### Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Wests Irondequoit Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
3. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
6. Address how the data will be protected using encryption while in motion and at rest.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the NYSED Chief Privacy Officer. Changes/Additions are also anticipated as NYSED releases further guidance documents.

Supplemental information describing third-party vendors engaged in data sharing and confidentiality agreements with West Irondequoit Central School District can be found at: <https://dpit.riconedpss.org/billofrights/02d9d2af98c045c501f3>.

**West Irondequoit Central School District**

**Data Privacy Supplemental Information**

Service Provider: \_\_\_\_\_ Cengage Learning \_\_\_\_\_ Date:  
\_\_\_\_\_ May 15, 2020 \_\_\_\_\_

What protected data is stored?

Please refer to our Privacy Statement at <https://www.cengage.com/privacy/notice/>.

For what purpose(s) will this data be used?

Please refer to our Privacy Statement at <https://www.cengage.com/privacy/notice/>.

What will happen to the data at the expiration of the contract/agreement?

Data will be appropriately disposed or returned based on the requirements under the Master Agreement.

How may the accuracy of data be challenged?

Please refer to our Privacy Statement at <https://www.cengage.com/privacy/notice/>.

Where is the data stored and how is it protected?


Please refer to our Privacy Statement at <https://www.cengage.com/privacy/notice/>. And also Exhibit 1: Cengage Learning Information Security Program Overview.

How is the data protected using encryption while in motion and at rest?

Please refer to Exhibit 1: Cengage Learning Information Security Program Overview.

**Provider Statement: We agree to abide by the terms above.**

Name: Jennifer Fritsch Title: VP Gale K12 Sales

Signature:  Date: 5/18/2020

## Exhibit 1

### Cengage Learning Information Security Program Overview

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

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

#### 1. Information Security Management

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

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

#### 2. Identification of Risks

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

#### 3. Formal Definition of an Information Security Policy

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

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

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

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

#### **4. Information Security Policy Review**

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

#### **5. Information Security Incident Response Plan**

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

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

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

#### **6. Third-Party Sub-contractors/Subprocessors**

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

The following entities are deemed approved as subprocessors:

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

#### **7. Audit and Assurance**

- Internal Audits and Internal Control Reports. Cengage conducts periodic vulnerability assessments to verify the sufficiency of its security measures. Cengage also engages third party auditors to review its security controls and may provide Client with a copy of applicable internal control reports (SOC Type II), which reports shall be classified as confidential information of Cengage.



- **Client Audits.** To the extent required by law, Cengage shall permit Client (or an independent third-party auditor for Client that is subject to confidentiality obligations) to audit Cengage's security practices relevant to Personal Data processed hereunder. Unless restricted by law, these audits are subject to the following terms:
  - (i) Client audits shall take place upon thirty (30) days advance notice to Cengage. Cengage shall work with Client in good faith to provide Client with the information needed to support such audit. Client and Cengage shall mutually agree to the scope and determine the agenda of the audit in advance. The audit shall, to the extent possible, rely on certifications and audit reports or other verifications available to confirm Cengage's compliance with the applicable security requirements.
  - (ii) Client may conduct a site visit of Cengage's facilities at Client's expense. Access at Cengage facilities shall be subject to Cengage's reasonable access requirements and security policies. The site visit is subject to the following conditions: (i) such site visit shall occur at a mutually agreeable time not more than once during any given calendar year; (ii) such site visit shall not unreasonably interfere with or disrupt Cengage's operations; and (iii) any third party performing such site visit on behalf of Client shall execute a nondisclosure agreement with Cengage in a form reasonably acceptable to Cengage with respect to the confidential treatment and restricted use of Cengage's confidential information, (iv) the scope of the site visit must be mutually agreed upon by the parties and shall exclude direct access to Cengage's systems, applications, network components, data center or testing of transactions.
- **Audit Findings.** If Client discovers a breach of Cengage's obligations, Client and Cengage shall work expeditiously and in good faith to agree on a plan to remediate such problems ("Remediation Plan"). Once the parties agree on a Remediation Plan, Cengage shall execute and complete the same without unreasonable delay and notify Client when such actions are completed. Notwithstanding the following, Cengage's shall have the sole discretion to determine which measures are best suitable to ensure compliance with applicable security requirements and laws.
- **Cooperation with Regulatory Audits.** Cengage shall fully cooperate with Client, at Client's expense, in connection with any governmental audit or investigation regarding Client's data or the data processing activities. (In the event that such audit or investigation is a result of Cengage's violation of applicable law, then Cengage shall be responsible for the costs and expenses or the audit or investigation).