

**CAZENOVIA**  
CENTRAL SCHOOL DISTRICT



**A TRADITION OF  
EXCELLENCE & EQUITY**

31 Emory Ave  
Cazenovia, NY 13421

JENNIFER RAUX  
Director of Instructional Technology

Phone: 315.655.1314, X.5380

**DATE: 9-13-23**

**To Whom it May Concern:**

RE: <The Digital SLP> Agreement with Cazenovia Central School District

The Cazenovia Central School District would like to contract with your company for the above referenced program/service. Attached you will find the agreement between your company and the Cazenovia Central School District concerning the NYS Ed Law and Regulations 121, Data Security and Privacy. Please review the agreement and return signed to Jennifer Raux, Director of Instructional Technology via email.

Sincerely,

Jennifer Raux  
Director of Instructional Technology, Data Protection Officer  
Cazenovia Central School District  
31 Emory Ave  
Cazenovia, NY 13035  
[jraux@caz.cnyric.org](mailto:jraux@caz.cnyric.org)  
315-655-1314 ext. 5380

# Cazenovia Central School District

## Data Security and Privacy Contract & Parents' Bill of Rights

Pursuant to Section 2-d of the Education Law, agreements entered into between the District and a third- party contractor which require the disclosure of student data and/or teacher or principal data that contains personally identifiable information ("PII") to the contractor, must include a data security and privacy plan and must ensure that all contracts with third-party contractors incorporate the District's Parents' Bill of Rights for Data Security and Privacy.

As such, Annotate.net ("the Contractor") agrees that the following terms shall be incorporated into the contract for services ("the Contract") and it shall adhere to the following:

1. The Contractor's storage, use and transmission of student and teacher/principal PII shall be consistent with the District's Data Security and Privacy Policy available here:
  - a. <http://go.boarddocs.com/ny/cazenovia/Board.nsf/goto?open&id=CBQJDW4CBE06>
2. Contractor shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.
3. The exclusive purposes for which the student data or teacher or principal data will be used under the contract are set forth in Paragraph 20-23 of the Vendor Privacy Policy/Contract only for the term of the Contract as set forth in the 2nd last paragraph or as summarized below.
4. The Contract shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which shall align with the NIST Cybersecurity Framework, including:
  - a. PII data will be protected using encryption while in motion and at rest. Please describe:

The Digital SLP has a comprehensive Security Program in place designed to protect the confidentiality, integrity and availability of systems, networks and data. The following is a general overview of data security protocols:

**Data in Transit:**

SSL-backed HTTPS for website access; SFTP for uploads.

**Data at Rest:**

List names are encrypted with the Defuse PHP Encryption library in the WordPress database. The encryption key is stored separately on the server filesystem. User passwords are protected by the WordPress password encryption algorithm.

- b. PII will be stored in a manner as to protect its security and to mitigate any potential security risks. Specifically, all student data and/or teacher or principal data will be stored as follows:

## Cazenovia Central School District

List names are stored in the database in an encrypted format using the Defuse PHP Encryption library. The key to decode the stored list is not saved in the database, so if the database is ever compromised or stolen, the list names cannot be decrypted without this key.

The key to decode the lists is kept in a separate location in the file system on the server, separate from the database.

The security of this data will be ensured by:

### Data Center Security:

The database is stored on the LiquidWeb dedicated server along with the files for the website. LiquidWeb provides an Acronis backup service which backs up to the LiquidWeb cloud storage on a daily basis. Additional backup data is stored within Dropbox Business; the database is encrypted before it is uploaded to Dropbox, and the website files are also stored there in zip form.

The website is hosted by Liquid Web in a high-security facility staffed 24/7/365 that is HIPAA/HITECH compliant.

<https://www.liquidweb.com/products/cloud-servers/>

## Cazenovia Central School District

- c. Physical access to PII by individuals or entities described in paragraph 3 above shall be controlled as follows:

The Digital SLP website is hosted on a physically secure, HIPAA/HITECH compliant server behind a hardware firewall, hosted by LiquidWeb.

All server access is protected by a physical Cisco firewall with only the required ports open for website access.

Website access is controlled via unique accounts for each person needing access to PII with two-factor authentication.

5. The Contractor shall ensure that no PII is disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Contract.

- a. By initialing here     *AC*    , the Contractor represents that it will not utilize any subcontractors or outside entities to provide services under the Contract and shall not disclose any PII other than as required pursuant to paragraph 6 below.
- b. If subcontractors are used, describe how the Contractor will manage data privacy and security:

Background Checks: All employees with access to student data have undergone criminal background checks.

Training: Employees of The Digital SLP will receive annual privacy and security training that includes FERPA.

Access: Access to student data is role-based; limited to those employees who need access to perform job responsibilities.

Employees are given access to the minimum services that are required for their job function.

6. Contractor shall ensure that all employees, subcontractors, or other persons or entities who have access to PII 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). Contractor shall provide training to any employees, subcontractors, or other persons or entities to whom it discloses PII as follows:

Training: Employees of The Digital SLP will receive annual training focused on privacy, FERPA

## Cazenovia Central School District

and security related items.

7. Contractor shall not disclose PII to any other party other than those set forth in paragraph 4 above without prior written parental consent or unless required by law or court order. If disclosure of PII is required by law or court order, the Contractor shall notify the New York State Education Department and the District no later than the time the PII is disclosed unless such notice is expressly prohibited by law or the court order.

## Cazenovia Central School District

8. Upon expiration of the contract, the PII will be returned to the District and/or destroyed. Describe below the transfer and/or destruction information (i.e., whether, when and in what format the data will be returned to the District, and/or whether, when and how the data will be destroyed.

The Digital SLP will retain and use users information as necessary to comply with their legal obligations only. They will retain user information only for as long as the account is active or as needed to provide services.


Unless the user requests that The Digital SLP delete certain information, they will retain the information collected for as long as the account is active or as needed to provide the services. Following termination or deactivation of the account, they will retain information for at least 3 years and may retain the information for as long as needed for business and legal purposes.

9. The parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected in accordance with the procedures set forth in the FERPA regulations at 99 C.F.R. Part 34, Subpart C, §§99.20-99.22.
10. The Contractor shall take the following steps to identify breaches or unauthorized releases of PII and to notify the District upon learning of an unauthorized release of PII. Minimum requirements are noted below in 10a, 10b and 10c.
  - a. Provide prompt notification to the District no later than seven (7) calendar days from date of discovery of a breach or unauthorized release of PII. Contractor shall provide notification to the District's data privacy officer by phone and by email.
  - b. Contractor shall cooperate with the District and law enforcement to protect the integrity of the investigation of any breach or unauthorized release of PII.
  - c. Where a breach or unauthorized release is attributed to the Contractor, the Contractor shall pay for or promptly reimburse the District for the full cost of such notification.
11. A complete list of all student data elements collected by the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
12. Parents have the right to file complaints with the District about possible privacy breaches of student data by the District's third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to [CPO@mail.nysed.gov](mailto:CPO@mail.nysed.gov).

## Cazenovia Central School District

### AGREED TO BY:

Organization: The Digital SLP, LLC


Contractor's Signature: 

Name: Jessica Cassity

Title: CEO/ Owner

Date: 09/19/2023

District: Cazenovia Central School District

Administrator's Signature: 

Name: Jennifer Raux

Title: Director of Instructional Technology

Date: 9-19-23

# Cazenovia Central School District

## PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM E

1. **EXCLUSIVE PURPOSES FOR DATA USE:** The exclusive purposes for which “student data” or “teacher or principal data” (as those terms are defined in Education Law Section 2-d and collectively referred to as the “Confidential Data”) will be used by **The Digital SLP** (the “”) are limited to the purposes authorized in the contract between the Vendor and Cazenovia Central School District (the “School District”) dated **9-19-23** (the “Contract”).
2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Vendor will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., Family Educational Rights and Privacy Act (“FERPA”); Education Law §2-d; 8 NYCRR Part 121).
3. **CONTRACT PRACTICES:** The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the School District **in a format agreed with the School District** format and/or destroyed by the Vendor as directed by the School District.
4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any “education record”, as that term is defined in the FERPA, stored by the School District in a Vendor’s product and/or service by following the School District’s procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by School District in Vendor’s product and/or service by following the appeal procedure in the School District’s APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.
5. **SECURITY PRACTICES:** Confidential Data provided to Vendor by the School District will be stored in encrypted form protected by SSL, stored in a secured HIPAA/HITECH compliant server located in a physically secured, monitored and staffed facility. Access to data is allowed via individual user accounts following the principle of least privilege.. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
6. **ENCRYPTION PRACTICES:** The Vendor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.