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. 8/14/23

To Whom it May Concern:
RE: CDW Government, LLC (CDWG) agreement with Cazenovia Central School District for Amplified IT Tools.

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.

Please note the following areas of the document that require your attention:

- Page 1 Service vs. License
- Page 1 Term of service
- Page 4 Signature
- Page 5 Addendum A
- Page 6-8 Addendum B
- Page 9 Addendum C
- Page 11 Addendum E
- Page 12-13 Addendum F

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

Software Vendor Education Law and Regulation 121 Agreement

Cazenovia Central School District

This Software Vendor Education Law and Regulation 121 Agreement ("Ed Law 121 Agreement"), together with Addenda A through [?] is made and entered into by and between CDW Government, LLC, having offices at 230 N. Milwaukee Avenue, Vernon Hills, IL, 60061 ("Vendor"), and the Cazenovia Central School District, having an office at 31 Emory Avenue, Cazenovia, New York 13035 ("School District") (collectively "Parties").

This Ed Law 121 Agreement is incorporated into, forms a part of, is applicable only to, the School District's Purchase Order issued to Vendor that includes Amplified IT SaaS Tools ("AIT Tools") and related professional services, numbered [231136] dated on or about [4/27/23 (the "Purchase Order"). The terms and conditions of Ed Law 121 Agreement apply only to the AIT Tools, and shall continue in force and effect coextensively with the School District's subscription to the AIT Tools that the School District acquires under the Purchase Order, and any renewals thereof.

By entering into this Ed Law 121 Agreement, the Parties understand and agree that the Amplified IT Tools are governed by the following sets of terms and conditions, each of which are incorporated into the Purchase Order:

Sourcewell 081419-CDW agreement
Amplified Labs Terms of Use
This Ed Law 121 Agreement

The foregoing documents, together with the Purchase Order, form the complete agreement for the products and services ordered under the Purchase Order. In the event of a conflict between any provision of this Ed Law 121 Agreement and the Sourcewell 081419 agreement or the Amplified Labs Terms of Use ("AIT Terms of Use"), the applicable provision of this Ed Law 121 Agreement shall prevail.

With respect to the AIT Tools purchased under the Purchase Order, the Parties agree as follows:

1. **Data Accessed by Vendor.** The School District has identified various categories of data in Addendum B. For each data category listed in Addendum B, Vendor has indicated, by checking the box labelled "Check if used by your system" whether such category of data is, or may be, accessed by Vendor or its subcontractors by the AIT Tools As such, the completed Addendum B contains the Confidential Information of CDWG.

2. **Protection of Confidential Data and Use by Contractor**.

2.1 Vendor shall provide its Services in a manner which protects Student Data (as defined by 8 NYCRR § 121.1(q)) and Teacher or Principal Data (as defined by 8 NYCRR § 121.1(r)) (hereinafter "Confidential Data") in accordance with applicable requirements articulated under Federal, State and local laws and regulations, including but not limited to the following:

(a) Vendor will adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework, as such Framework is defined in NYCRR 121.1 (k).

(b) Vendor will comply with applicable provisions of the School District Data Security and Privacy Policy, Education Law § 2-d, and 8 NYCRR § 121.

(c) Vendor will limit internal access to personally identifiable information (as defined in 8 NYCRR § 121.1 (m)) ("PII") to only those employees or subcontractors that need such access to provide the contracted services.

(d) Vendor will not use the PII for any purpose not explicitly authorized in this Ed Law 121 Agreement.

(e) Vendor will not disclose any student PII to any other party without the prior written consent of the parent or eligible student, unless otherwise authorized pursuant to applicable law.

(f) Vendor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody.

(g) Vendor will use encryption to protect PII in its custody while in motion or at rest.

(h) Vendor will not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i) In the event Vendor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Vendor shall apply to the subcontractor.

2.2 **Authorized Use of Confidential Data by Vendor**

Vendor shall use any student data, teacher data, or principal data accessed by the AIT Tools for the exclusive purposes of: a) providing the SaaS and related professional services ordered by the School District under the Purchase Order (and any renewals or extensions thereof); b) facilitating the provision of support to the School District and its users relating to the AIT Tools; and c) creating updates to its products and services and improving its products and technologies, provided that the information is used in a form that does not personally identify the School District or any individual student, teacher, or principal.

3. **Data Breach**. In the event that Vendor becomes aware that the School District's Confidential Data residing within Vendor's systems or transiting through the AIT tools (as defined in Section 2 hereof) has been accessed, used, disclosed or obtained by an unauthorized party ("Data Breach"), Vendor shall provide notification to the School District without unreasonable delay and not more than seven (7) calendar days after the discovery of such breach. Vendor shall follow the following process:

(a) The data breach notification shall be titled "Notice of Data Breach," shall be clear, concise, use language that is plain and easy to understand, and to the extent available, shall include: a brief description of the breach or unauthorized access; the dates of the incident and the date of discovery; a description of the types of Confidential Data affected; an estimate of the number of records affected; a brief description of the Vendor's investigation or plan to investigate; and contact information for representatives who can assist the School District with additional questions. Any Notice of Data Breach shall be deemed the Confidential Information of the Vendor.

(b) If Student Data (as defined above) is affected by the Data Breach, the Vendor shall also prepare a statement for parents and eligible students, to be distributed by the School District in its discretion, which provides information under the following categories: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Any School District changes to the Vendor-drafted statement shall be mutually agreed between the Vendor and the School District.

(c) Where a Data Breach of Confidential Data is proximately caused by the gross negligence, willful misconduct, or violation of law of Vendor, and/or a subcontractor or affiliate of Vendor, Vendor shall pay for or promptly reimburse the School District for the reasonable cost of notification to parents and eligible students of the breach.

(d) Vendor shall cooperate with the School District and law enforcement to protect the integrity of investigations into the Data Breach or unauthorized release of Confidential Data.

(e) Vendor further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and Federal and State laws for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Confidential Data or any portion thereof. Upon request, Vendor shall provide a copy of said written incident response plan to the School District. Vendor's incident response plan is deemed the Confidential Information of the Vendor.

8. **Indemnification**. Vendor shall at all times (both during and after the Term of this Agreement), indemnify, defend and hold harmless the School District, its agents, employees, and students (collectively for purposes of this Section, "the School District"), from and against any and all third party claims arising from Vendor's failure to comply with the terms of this Ed Law 121 Agreement..

14. **Addendums.** The following Addenda are attached hereto and incorporated herein:

- Addendum A: Description of Specifications and Services
- Addendum B: Schedule of Data
- Addendum C: RESERVED
- Addendum D: School District's Parents' Bill of Rights
- Addendum E: Parents' Bill of Rights – Supplemental Information Addendum
- Addendum F: Vendor's Data Security and Privacy Plan
- Addendum G: Data Privacy and Security Privacy Policy - Cazenovia CSD

IN WITNESS WHEREOF, the Parties have signed this Agreement intending to be legally bound.

<Vendor> CDW GOVERNMENT LLC	**Cazenovia Central School District**
By:	By: *Jennifer Raux*
Name: Dario Bertocchi	Name: Jennifer Raux
Title: VP Contracting Operations	Title: Director of Instructional Technology
Date: Aug 18, 2023	Date: 8/14/23

Addendum A: Description Of Specifications And Services

Description of SaaS Services

Amplified IT Tools subscriptions: (1) Gopher and (2) Little Sis

SaaS Service Specifications

As set forth in documentation

Gopher for Chrome allows Chrome device data to be imported, filtered, analyzed. Update, deprovision, or disable/enable from Sheets.

Little SIS Premium is a powerhouse Cloud-based product that makes Google Classroom management even more efficient and effective.

SaaS Service Technical Specifications

As set forth in documentation

Addendum B: Schedule of Data

THIS SCHEDULE CONTAINS THE <u>CONFIDENTIAL AND PROPRIETARY INFORMATION OF CDWG, LLC.</u>

Category of Data	Elements	Check if used by your system
Application of Technology Metadata	IP Addresses, Use of cookies, etc.	GfC
	Other application technology metadata (specify):	N/A
Application Use Statistics	Metadata on user interaction with applications	GfC
Assessment	Standardized test scores	N/A
	Observation data	N/A
	Other assessment data (specify):	N/A
Communications	Online communications that are captured (emails, blog entries)	N/A
Conduct	Conduct or behavioral data	N/A
Demographics	Date of Birth	N/A
	Place of Birth	N/A

	Gender	N/A
	Ethnicity or race	N/A
	Language Information (native, preferred or primary language spoken by student)	N/A
	Other Demographic information (specify):	N/A
Enrollment	Student school enrollment	N/A
	Student grade level	N/A
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
	Year of graduation	N/A
	Other enrollment information (specify):	N/A
Parent/Guardian Contact Information	Address	N/A
	Email	N/A
	Phone	N/A
Parent/Guardian ID	Parent ID Number (created to link parents to students)	N/A
Parent/Guardian Name	First and/or last	N/A

Schedule	Student scheduled courses	N/A
	Teacher Names	N/A
Special Indicator	English Language Learner information	N/A
	Low income status	N/A
	Medical alerts	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information (specify):	N/A
Student Contact Information	Address	N/A
	Email	GfC
	Phone	N/A
Student Identifiers	Local (School DIstrict) ID number	N/A
	State ID number	N/A
	Vendor/App assigned student ID number	GfC
	Student app username	GfC

	Student app passwords	N/A
Student Name	First and/or Last	GfC
Student In-App Performance	Program/application performance (ex: typing program-student types 60 wpm, reading program-student reads below grade level)	N/A
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	Student responses to surveys or questionnaires	N/A
Student Work	Student generated content, writing, pictures, etc.	N/A
	Other student work data (please specify):	N/A
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/performance scores	N/A
	Other transcript data (please specify):	N/A
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A

	Student bus card ID number	N/A
	Other transportation data (please specify):	N/A
Other	Please list each additional data element used, stored or collected by your application	N/A

Addendum C: RESERVED

Addendum D: Cazenovia Central School District Parents' Bill Of Rights

The School District's Parent's Bill of Rights is included herein as Addendum D, for informational and reference purposes, and as required by 8 NYCRR § 121.3(b).

EDUCATION LAW §2-D BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) of the Cazenovia Central School District can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacy security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Addendum E: Parents’ Bill Of Rights – Supplemental Information Addendum

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 CDW Government, LLC (the “Vendor”) are limited to the purposes authorized in the contract between the Vendor and Cazenovia Central School District (the “School District”) dated <**contract date**> (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 § 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. Thirty days following expiration or termination of the District’s subscription for the applicable AIT Tool, any data stored in Vendor servers in connection with the School District’s or its users’ use of the AIT Tools, including any protected data, will be deleted from Vendors’ servers.

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 the United States. 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.

Addendum F: Vendor’s Data Security and Privacy Plan

THIS ADDENDUM CONTAINS THE <u>CONFIDENTIAL AND PROPRIETARY INFORMATION OF CDWG, LLC.</u>

WHEREAS, the Cazenovia Central School District (hereinafter "School District") and <**CDWG**> (hereinafter "Contractor") entered into an agreement dated <**8/14/23**> (hereinafter "Agreement") for **services** (hereinafter "Services").

WHEREAS, pursuant to the requirements under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

1. During the term of the Agreement, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the School District's Data Security and Privacy Policy in the following way(s):

Any and all user and customer data used in the provision of the services outlined is retrieved from Google Workspace and is held in accordance with our data security and privacy policies to ensure limited and secure access.

This data is never sold or passed on to a third party.

Following delivery of services, this data can and will be removed from CDW system as outlined above.

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement:

CDW thoroughly understands and prioritizes its mission, objectives, stakeholders, and business activities, utilizing this information to inform decision-making processes related to cybersecurity roles, responsibilities, and risk management. As such, CDW ensures that appropriate measures are implemented to safeguard critical assets, address potential vulnerabilities, and effectively manage cybersecurity risks in a manner that supports our mission and objectives.

3. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the School District's Parents Bill of Rights for Data Privacy and Security and will comply with same.
    a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.
    b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the "Supplemental Information" appended to the Agreement.

c. At the end of the term of the Agreement, Contractor will destroy, transition or return, at the direction of the School District, all student data and all teacher and principal data in accordance with the "Supplemental Information" appended to the Agreement.

d. Student data and teacher and principal data will be stored in accordance with the "Supplemental Information" appended to the Agreement.

e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided: Specify date of each training

Employees of the contractor are required to take yearly cybersecurity training that covers the safeguarding of customer PII. Training is ongoing and is annual for each employee.

5. Subcontractors (check one):

- Contractor shall not utilize subcontractors.
- Contractor shall utilize subcontractors. Contractor shall manage the relationships and contracts with such subcontractors in the following ways in order to ensure personally identifiable information is protected:

Contractor shall not use subcontractors.

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information: Procedures, plans or protocols must, at a minimum, specify plans to identify breaches and unauthorized disclosures, and to promptly notify the School District.

CDW has established a robust governance framework that encompasses policies, procedures, and processes to effectively manage and monitor the organization's large variety of risk areas (e.g., regulatory, legal, operational). These requirements are thoroughly reviewed and play a crucial role in informing cybersecurity risk management activities. As such, CDW ensures that cybersecurity risks are appropriately identified, assessed, and mitigated--enabling compliance with applicable regulations and standards while safeguarding the organization's assets and operations.

7. Termination of Agreement.

a. Within 30 days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession;

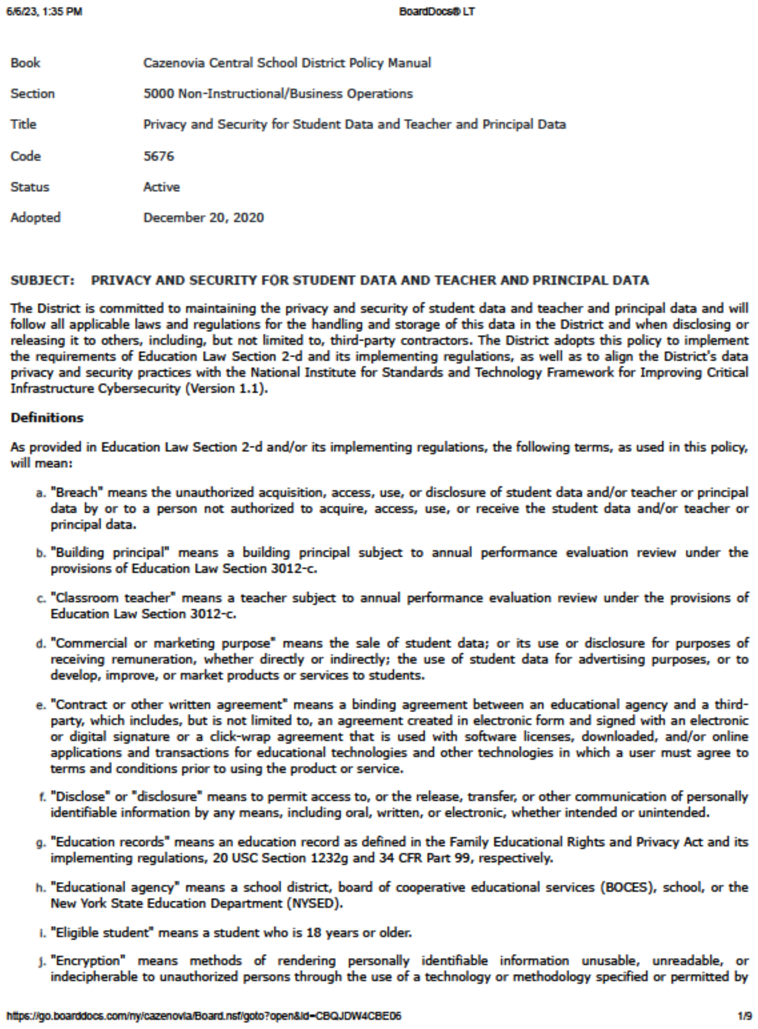
8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Ed Law 121 Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Ed Law 121 Agreement shall have the same definitions in the Data Security and

Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Ed Law 121 Agreement shall remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Contractor hereto has executed this Data Security and Privacy Plan as of <**8/14/23**>.

Contractor	CDW GOVERNMENT LLC
By	
Title	VP Contracting Operations

Addendum G: Data Privacy and Security Privacy Policy- Cazenovia CSD



6/6/23, 1:35 PM BoardDocs® LT

Book	Cazenovia Central School District Policy Manual
Section	5000 Non-Instructional/Business Operations
Title	Privacy and Security for Student Data and Teacher and Principal Data
Code	5676
Status	Active
Adopted	December 20, 2020

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA

The District is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the District and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The District adopts this policy to implement the requirements of Education Law Section 2-d and its implementing regulations, as well as to align the District's data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

a. "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

b. "Building principal" means a building principal subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

c. "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

d. "Commercial or marketing purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve, or market products or services to students.

e. "Contract or other written agreement" means a binding agreement between an educational agency and a third-party, which includes, but is not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement that is used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

f. "Disclose" or "disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

g. "Education records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

h. "Educational agency" means a school district, board of cooperative educational services (BOCES), school, or the New York State Education Department (NYSED).

i. "Eligible student" means a student who is 18 years or older.

j. "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by

https://go.boarddocs.com/ny/cazenovia/Board.nsf/goto?open&id=CBQJDW4CBE06 1/9

EDUCATION LAW §2-D BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacy security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

V1_06052020