

Attachment A – Parents’ Bill of Rights for Data Security and Privacy

Delaware-Chenango-Madison-Otsego BOCES Parent’s Bill of Rights for Data Privacy and Security

DCMO BOCES Parents’ Bill of Rights for Data Privacy and Security

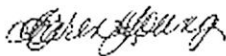
DCMO BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students’ education experience in the district, to enhance the opportunities for learning and to increase the efficiency of our district and school operations.

DCMO BOCES seeks to insure that parents have information about how the District stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, DCMO BOCES has posted this Parents’ Bill of Rights for Data Privacy and Security.

- (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. The procedures for exercising this right can be found in Board Policy 601. You may access this Policy from the District’s website.
- (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 the State is available at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 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 the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

For Vendor Name



Date: April 23, 2024

Name: Karen Young

Title: CEO

	Education Law Section 2-d, that challenge shall be processed through the appeal process, if any, in the APPR Plan of the employing educational agency.
SECURITY PRACTICES	<p>The data is stored in the continental United States (CONUS) or Canada.</p> <p>Vendor will maintain administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, and that align with the NIST Cybersecurity Framework 1.0. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2).</p>

Attachment C – Vendor’s Data Security and Privacy Plan

Data Security and Privacy Plan (COPY)

Effective January 1, 2020

For all New York State school and district work, A+ Educators DBA Woz ED officers and employees must keep any personally identifiable student information in password protected accounts that only the relevant team members can access. Personally identifiable information is not to be shared with any subcontractors. All subcontractors will be given anonymized information to maintain data security and privacy.

Specific team members must access data and information through a password protected account. This information is protected through Transport Layer Security. Only training and support staff working directly with the Educational Agency which owns the information may have access to that information.

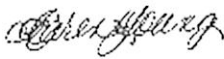
Officers and employees may only have access to Protected Data after successful completion of training on the federal and state laws governing confidentiality of such data related to the PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY in New York state and 100% accuracy on the corresponding multiple choice and short answer assessment. Original source documents associated with these regulations are accessible to all team members on the shared server.

Team members with access to this data will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and provide prompt notification of any breaches or unauthorized disclosures of Protected Data to an officer of the company, who will then notify the necessary Education Agency authorities.

Internal access to education records is limited to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA). This includes only those employees or subcontractors that need access in order to assist the company in fulfilling one or more of its obligations. No employee or subcontractor may use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement. Employees and officers may not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor’s obligations unless the parent or eligible student has provided prior written consent or the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

A+ Educators DBA Woz ED officers and employees will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student data.

Acknowledged:



Signature

Karen Young

Printed Name and Title

April 23, 2024 - Date