



DATA SECURITY AND CONFIDENTIALITY AGREEMENT

This DATA SECURITY AND CONFIDENTIALITY AGREEMENT ("Data Agreement") is entered into this .
04/12 day of y by and between MESA PUBLIC SCHOOLS ("District") and digiCOACH, Inc., and its
subcontractors and agents ("Service Provider").

RECITALS

- A. In providing services to the District, the Service Provider may have access to confidential records, data and information concerning students and employees of the District.
- B. Service Provider agrees to the terms and conditions of this Data Agreement and to adhere to the requirements of all relevant state and federal laws, which may be amended from time to time, and which the parties agree are incorporated herein by reference as currently existing or as amended, with respect to the receipt, review, storage, and transmission of data, records, and information received from the District.
- C. This Data Agreement shall be in addition to any underlying agreement for goods or services between the parties.

NOW, THEREFORE, THE PARTIES HEREBY AGREE AS FOLLOWS:

1. Covered Data and Information. All records, information, and data of the District to which Service Provider has access are hereafter referred to as "CDI". CDI includes but is not limited to, all records, information, data, and metadata, including student education records, supplied by the District or its students, employees, agents, board members, contractors, or any other entity for or on the District's behalf.

2. Compliance with all Applicable Laws and Regulations. Service Provider agrees to comply with all applicable laws and regulations regarding data/information/records security and privacy, all of which are incorporated herein by reference in their current forms and as amended at any future time. These include, but are not limited to, Arizona Revised Statute ("A.R.S.") §§ 15-141 (incorporation of FERPA into Arizona law), 18-501 to 18-552 (including notification of security system breaches); A.R.S. § 44-7601 (discarding and disposing of records containing personal identifying information); 20 U.S.C. § 1232g and 34 CFR Part 99, the Family Educational Rights and Privacy Act (FERPA); Protection of Pupil Rights Amendment (PPRA); Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Privacy and Security Rules; Health Information Technology for Economic and Clinical Health (HITECH) Act; Payment Card Industry Data Security Standards; applicable regulations of the Arizona Department of Education relating to the confidentiality of student records; and any other federal and/or state law governing the privacy of CDI.

3. Access and Use of CDI. Service Provider hereby acknowledges that they have access to CDI and that such access and use is the subject of this Data Agreement. Service Provider will only access, possess and use CDI as necessary to fulfill its duties as agreed to in any underlying agreement for goods or services. Service Provider agrees to comply with all District information security policies, standards and procedures when accessing District networks and computerized systems whether onsite or remotely. Service Provider will approve and track access to ensure proper usage and accountability.

4. Data Mining. Service Provider is prohibited from mining CDI for any purposes other than as agreed to in writing between the parties. Data mining or scanning of user content for the purpose of advertising or marketing to anyone is prohibited. Service Provider will not use any CDI, whether or not aggregated or de-identified, for product development, marketing, profiling, benchmarking or product demonstrations, or any other use without, in each case, express written permission of the District.

5. Confidentiality of CDI. Service Provider agrees to hold CDI in strict confidence. Service Provider shall not use or disclose CDI received from or on behalf of the District except as permitted or required by this Data Agreement, as required by law, or as otherwise authorized in writing by the District. Service Provider agrees that it will protect CDI it receives from or on behalf of the District according to commercially acceptable standards and no less rigorously than it protects its own confidential information.

6. Encryption. All systems and devices that receive, store, process or transmit CDI shall use the latest, advanced and highly secured industry-standard encryption protocol for data in transit and at rest.

7. Data De-Identification. Service Provider may have permission via an underlying agreement with the District to use de-identified CDI for the purpose(s) authorized by that agreement. De-identified CDI shall have all direct and indirect personal identifiers removed. This includes but is not limited to, name, identification numbers, date of birth, demographic information, location information and school identification numbers. Service Provider agrees not to attempt to re-identify de-identified CDI and agrees not to transfer de-identified CDI to any third party without the express written permission of the District. Any third party shall agree in writing not to attempt re-identification and shall agree to be bound to the same terms of this Data Agreement.

8. Reporting Student CDI. Service Provider may at times have reason to report CDI of District students to third parties as provided by express written permission from the District or as required by law. In reporting aggregated, de-identified data containing CDI, the Service Provider shall:

- a. Not disclose data about categories of 10 or fewer students;
- b. Not report a total count of students;
- c. Not report percentages of 0% or 100%; and
- d. Report data in ranges rather than specific numbers.

9. Destruction of CDI. Upon termination, cancellation, expiration or other conclusion of the work or services provided to the District by the Service Provider, the Service Provider shall destroy CDI, regardless of its format, within 30 days. When CDI is no longer needed for the specified purposes as authorized by the District, Service Provider shall ensure that all CDI in its possession or in the possession of any subcontractors or agents is destroyed through appropriate and secure methods that ensure the information cannot be viewed, accessed, or reconstructed. Service Provider should use NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization as a guideline in making data disposal and sanitization decisions. Service Provider shall take reasonable measures to protect against unauthorized access to or use of CDI in connection with its disposal. Destruction of CDI shall include redaction, destruction, erasure or other disposal of paper documents and electronic media so that these

types of information cannot be practicably read or reconstructed. Service Provider shall share policies and procedures regarding redaction, destruction, erasure, or other disposal methods with the District upon request. Service Provider shall confirm in writing to the District that it has destroyed all CDI and no longer has any CDI in its possession or control.

10. Security of Electronic Information. Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures and technical safeguards to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted CDI received from or on behalf of the District or its students or employees. Service Provider shall store and process CDI in accordance with current industry practices to secure CDI from unauthorized access, disclosure and use. These security measures and technical safeguards shall be extended by express written agreement to all subcontractors and third parties used by Service Provider. Service Provider shall at a minimum:

- a. Protect and maintain the confidentiality of passwords used to access CDI;
- b. Carry out updates and patch management for all systems and devices in a timely manner and to the satisfaction of the District, using an auditable process that can be reviewed by the District upon request;
- c. Notify the District when Service Provider's access to CDI is no longer necessary;
- d. Notify the District of all subcontractors or other third parties with access to the CDI through or on behalf of Service Provider, the level of such access and any subsequent changes in such access; and
- e. Notify the District when a subcontractor or third party no longer will have access to the CDI and confirm, in writing, that the subcontractor or third party has no CDI in its possession and no longer has access to the CDI.

If Service Provider's procedures and controls it uses to protect its own confidential information are more robust than the minimum requirements listed above, Service Provider agrees to use the same procedures and controls it uses to protect its own confidential information to protect the District's CDI.

Service Provider will conduct periodic risk assessments, at a minimum of once per year, and remediate any identified security vulnerabilities in a timely manner. If, at any time during the duration of this Data Agreement, the District determines that the procedures and controls in place are not adequate, Service Provider shall institute any new and/or additional measures requested by the District within fifteen business days of the written request to do so.

11. Reporting Unauthorized Disclosure, Breach or Misuse of CDI. Service Provider shall immediately, and under no circumstances more than seventy-two hours following its discovery, report to the District any breach of any system containing CDI, unauthorized use or disclosure of CDI (including, but not limited to, unauthorized disclosure of CDI, network intrusions, successful virus attacks, unauthorized access or modifications, and threats and vulnerabilities) of Service Provider and its subcontractors. Service Provider's report shall identify:

- a. The nature of the breach, unauthorized use or disclosure;
- b. The CDI accessed, used or disclosed;
- c. The identity of the person or entity who breached the system, made the unauthorized use or received the unauthorized disclosure;
- d. What Service Provider or subcontractor, as applicable, has done or will do to mitigate any deleterious effect of the unauthorized use or disclosure; and
- e. What corrective action Service Provider or subcontractor, as applicable, has taken or shall take to prevent further similar unauthorized use or disclosure.

Service Provider shall provide such other information, including a written report, as reasonably requested by the District. Service Provider shall have a plan for responding to a breach of data security developed pursuant to best practices in the industry and shall share that plan with the District upon request.

12. Reimbursement of Costs in Instance of Breach. Service Provider agrees to reimburse the District for any and all costs incurred by the District to investigate, respond to, and/or resolve any breaches, potential breaches, unauthorized access, use, or transfer of data by Service Provider or any subcontractor of a Service Provider, including but not limited to, where applicable, the cost of notifying individuals who may be impacted by the breach, attorneys' fees, and any monetary damages or penalties the District may be assessed.

13. District Access. Any CDI held by Service Provider will immediately be made available to the District upon request.

14. Data Ownership. The District will own, or retain all of its rights in, all CDI that the District provides to Service Provider, as well as all CDI managed by Service Provider on behalf of the District including output, analyses, and other materials relating to or generated by services provided even if generated by Service Provider or extracted by Service Provider from District systems. All CDI, regardless of form, including originals, images and reproductions prepared by, obtained by, or transmitted to Service Provider in connection with this Data Agreement is confidential, proprietary information owned by the District.

15. Rights to Intellectual Property. The parties agree that all rights, including all intellectual property rights, shall remain the exclusive and sole property of the District and that Service Provider has a limited, non-exclusive license solely for the purposes of performing its obligations as outlined in any underlying agreement for goods or services. This Data Agreement does not give Service Provider any rights, implied or otherwise, to CDI, data, content or intellectual property except as expressly stated in any underlying agreement between the parties. This includes but is not limited to the right to sell or trade CDI.

16. Insurance. Service Provider, without limiting any liabilities or any other obligations, shall procure and maintain, until all of their obligations have been discharged, including any warranty periods under this Data Agreement, insurance against claims in connection with the performance of work from this Data Agreement by the Service Provider, its agents, representatives, employees or subcontractors. Service Provider shall provide proof of coverage with limits of liability not less than those stated below.

Network Security (cyber) and Privacy Liability insurance with minimum limits of \$2,000,000 per claim and \$2,000,000 annual aggregate, with the following requirements:

- Policy shall name Mesa Public Schools as an additional insured;
- Policy shall contain no requirements for arrest and conviction;
- Policy shall cover loss outside the premises of the Named Insured;
- Policy shall include, but not be limited to, coverage for third party claims and losses with respect to network risks (such as data breaches, unauthorized access or use, ID theft, theft of data) and invasion of privacy regardless of the type of media involved in the loss of private information, crisis management and identity theft response costs; and
- Policy shall include breach notification costs, credit remediation and credit monitoring, defense and claims expenses, regulatory defense costs plus fines and penalties, cyber extortion, computer program and electronic data restoration expenses coverage (data asset protection), network business interruption, computer fraud coverage, and funds transfer loss.

17. Indemnity. Service Provider shall defend and hold the District, its Board Members, officers, agents and employees, harmless from all claims, liabilities, damages or judgments involving a third party, including the District's costs and attorneys' fees, which arise as a result of Service Provider's failure to meet any of its obligations under this Data Agreement.

18. Remedies. If the District determines in good faith that Service Provider has materially breached any of its obligations under this Data Agreement, the District shall have the right to require Service Provider to submit to a plan of monitoring and reporting; to provide Service Provider with a fifteen (15) day period to cure the breach; or to terminate the work or services of Service Provider for the District immediately. Prior to exercising any of these options, the District shall provide written notice to Service Provider describing the violation and the action the District intends to take. The remedies described herein may be exercised by the District in its sole discretion and are in addition to any remedies permitted by law or pursuant to any other agreement between the parties.

19. Subcontractors. Service Provider shall require that any subcontractor or agent receiving CDI is authorized by the District in writing to receive CDI and that the subcontractor or agent expressly agrees to be bound by the same the terms of this Data Agreement.

20. Offshore Services. Direct services under this Data Agreement shall be performed within the borders of the United States. Any services that are described in this Data Agreement that directly serve the District and may involve access to secure or sensitive CDI or development or modification of software for the District shall be performed within the borders of the United States. Unless stated otherwise, this requirement does not apply to indirect or "overhead" services, redundant back-up services or services that are incidental to the performance of this Data Agreement. This provision applies to work performed by subcontractors at all tiers for all CDI.

21. Outside Requests for CDI. Service Provider shall immediately notify the District if Service Provider receives any kind of subpoena for or involving CDI, if any third-party requests CDI, or if Service Provider has a change in location or transmission of CDI. All notifications to the District required under this paragraph shall be sent to the District: **Chief Privacy Officer, 63 E. Main Street, Mesa, AZ 85201**. Under no circumstances shall Service Provider disclose or provide CDI to any third party without first notifying the District in writing and giving the District reasonable time to object to such disclosure.

22. Modifications. Service Provider will not modify or change how CDI is collected, used or shared under the terms of this Data Agreement in any way without advance written notice to and consent from the District.

23. Arizona Law. This Data Agreement is made in the State of Arizona and shall be interpreted and governed by the laws of the State of Arizona. Any dispute arising out of or relating to this Data Agreement shall be brought in the Maricopa County Superior Court or the United States District Court, District of Arizona.

24. Term. This Data Agreement shall take effect upon execution by all parties and shall continue until the expiration of any underlying agreement, if applicable, or until it is terminated in writing or superseded by a new Data Agreement.

25. Cancellation. The District reserves all rights that it may have to cancel this Data Agreement for possible conflicts of interest under ARS § 38-511, as amended.

26. Miscellaneous. The provisions of this Data Agreement shall survive the termination, cancellation or completion of all work, services, performances or obligations by Service Provider to the

District. This Data Agreement shall be binding upon the parties hereto, their officers, employees and agents. Time is of the essence of this Data Agreement. Except as expressly modified by provisions of this Data Agreement, any underlying agreement for goods or services shall continue in full force and effect. In the event any inconsistencies exist between the terms of this Data Agreement and any underlying agreement, this Data Agreement shall control.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed by its authorized parties on its behalf.

MESA PUBLIC SCHOOLS

By: 

Its: Nathan Myers

Date: 12/04/24

VENDOR NAME

By: 
Wesley Whittaker (Dec 4, 2024 09:49 PST)

Its: Wesley Whittaker

Date: 12/04/24

Signature: 

Email: nmsietsema@mpsaz.org











MPS EMPLOYEE DATA SECURITY AND CONFIDENTIALITY AGREEMENT

Final Audit Report

2024-12-04

Created:	2024-12-03
By:	Educational Technology (edtech@mpsaz.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAEqS9O8LhkSaqUarWFNVReObRnLKzSD6H

"MPS EMPLOYEE DATA SECURITY AND CONFIDENTIALITY AGREEMENT" History

-  Document created by Educational Technology (edtech@mpsaz.org)
2024-12-03 - 10:49:23 PM GMT
-  Document emailed to wes@digicoach.com for signature
2024-12-03 - 10:53:44 PM GMT
-  Email viewed by wes@digicoach.com
2024-12-04 - 5:48:52 PM GMT
-  Signer wes@digicoach.com entered name at signing as Wesley Whittaker
2024-12-04 - 5:49:23 PM GMT
-  Document e-signed by Wesley Whittaker (wes@digicoach.com)
Signature Date: 2024-12-04 - 5:49:25 PM GMT - Time Source: server
-  Document emailed to Nichole Sietsema (nmsietsema@mpsaz.org) for signature
2024-12-04 - 5:49:26 PM GMT
-  Email viewed by Nichole Sietsema (nmsietsema@mpsaz.org)
2024-12-04 - 9:30:04 PM GMT
-  Document e-signed by Nichole Sietsema (nmsietsema@mpsaz.org)
Signature Date: 2024-12-04 - 9:30:43 PM GMT - Time Source: server
-  Document emailed to Nathan Myers (namyers@mpsaz.org) for signature
2024-12-04 - 9:30:44 PM GMT
-  Document e-signed by Nathan Myers (namyers@mpsaz.org)
Signature Date: 2024-12-04 - 11:47:36 PM GMT - Time Source: server

✔ Agreement completed.

2024-12-04 - 11:47:36 PM GMT



Adobe Acrobat Sign