Scottsdale Unified School District #48

DATA SECURITY AND CONFIDENTIALITY AGREEMENT

This DATA SECURITY AND CONFIDENTIALITY AGREEMENT ("Data Agreement") dated August 31st, 2022, by and between Scottsdale Unified School District #48 (the "District') and Amplify Education, Inc. (the "Service Provider"). Service provider assumes full responsibility for its agents and subcontractors, if any.

RECITALS

A. In providing services to the District, Service Provider may have access to confidential records, data and information concerning students and employees of the District.

B. Service Provider agrees to the provisions of this Data Agreement and to the requirements of state and federal law with respect to the receipt, review, storage and transmission of information received from the District.

C. This Data Agreement shall be in addition to any underlying agreement for goods and services entered into 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 paper and electronic student education records, information and data supplied by the District, as well as any such records, information and data provided by students of the District, all personally identifiable records, information and data concerning students and employees of the District, and all personally identifiable information (" PII") and other non-public information supplied, including but not limited to student data, employee data, and user content.

2. Limited Use of De-identified, aggregate or anonymized CDI. CDI does not include deidentified, aggregate or anonymized CDI (collectively "De-Identified Data"). The District permits the Service Provider to use de-identified, aggregate or anonymized CDI for purposes permitted by FERPA and the purpose of research and development to improve the service offered by the Service Provider. Service Provider may not transfer any de-identified, aggregate or anonymized CDI to a third party without the express written consent of the District unless that party has agreed in writing not to attempt to re-identify such De-Identified Data.

3. Compliance with all Applicable Laws. Service Provider agrees to comply with the requirements of The Family Educational Rights and Privacy Act (FERPA), the Pupil Protection Rights Act (PPRA), and any other federal and/or state law governing the privacy of CDI. If Service Provider processes data outside of the United States, Service Provider specifically agrees to be bound by A.R.S. § 18-551. and -552, as amended, A.R.S. § 15-241, FERPA, PPRA and any other applicable Arizona or federal law governing CDI.

4. Access to CDI. Service Provider hereby acknowledges that the Service Provider has access to CDI and that such shall be subject to the terms and conditions of this Data Agreement. Service Provider will only collect CDI as necessary to fulfill its duties as agreed to in any underlying agreement for goods or services.

5. Use of CDI. Service Provider will use CDI only for the purpose of fulfilling its duties and providing services as agreed to in any underlying agreement for goods or services.

6. 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 to advertise or market to anyone without express written permission of the District.

7. 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, as necessary to provide the goods or services pursuant to the underlying agreement, 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.

8. Data De-Identification. Service Provider may have permission via any underlying agreement to provide goods or services to use de-identified CDI for purposes as identified in the agreement. CDI is considered to be de-identified when all PII has been removed or obscured, such that the remaining information does not reasonably identify a specific individual. Service Provider will de-identify student CDI in compliance with applicable laws and in accordance with the guidelines of NIST SP 800-122.Service Provider agrees not to attempt to re-identify de-identified CDI and, unless that party has agreed in writing not to attempt to re-identify such De-Identified Data, agrees not to transfer de-identified CDI to any party without permission.

9. 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.

10. Return or Destruction of CDI. Service Provider shall delete CDI at any time within ninety (90) days of receipt of request by the District. The District is responsible for maintaining current class rosters and notifying Service Provider to destroy CDI which the District no longer needed for the purposes of this DPA. Upon termination of this DPA, if no such notification is received, Service Provider shall destroy CDI after a period of at least one year of inactivity, in accordance with Service Provider's standard data retention policies and procedures. If requested, Service Provider will transfer CDI to the District in a mutually agreeable format. Additionally, upon such request for deletion or such period of inactivity, Service Provider shall ensure that all CDI in the possession of any subcontractors or agents is destroyed or returned to the District.

11. 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 industry standard practices to secure CDI from unauthorized access, disclosure and use. Service Provider accepts full responsibility for the efforts of its agents and/or subcontractors, if any, to use such measures, safeguards, and practices.Service Provider shall at a minimum:

    a. Protect and maintain the confidentiality of passwords used to access CDI;

    b. Discontinue access upon receipt of notification from the District when Service Provider's access to CDI is no longer necessary;

    c. Notify the District as soon as reasonably possible, and in accordance with applicable laws, after discovery if passwords used to access CDI by Service Provider, a subcontractor, or other third party are lost, stolen, or otherwise obtained by unauthorized users.

    Service Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

12. Reporting of Disclosure or Misuse of CDI. Service Provider's breach notification obligations will be governed by Exhibit A, attached hereto.

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

14. Rights to Intellectual Property. This Data Agreement does not give Service Provider any rights, implied or otherwise, to the District's 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 share, sell or trade CDI. The District acknowledges that this agreement does not convey any intellectual property right in any of Service Provider's materials or content, including any revisions of derivative work or material. Service Provider-owned materials shall remain the property of the Service Provider. All rights, including copyright, trade secrets, patent and intellectual property rights shall remain the sole property of the Service Provider.

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

16. 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 thirty (30) day period to cure the breach; or to terminate the work or services of Service Provider for the District if such breach is not cured. 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.

17. Subcontractors. Service Provider shall require that any subcontractor or agent receiving CDI is authorized by the District to receive CDI and that the subcontractor or agent expressly agrees to be bound to terms no less stringent than the terms of this Data Agreement.

18. 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 notice to and consent from the District.

19. Arizona Law. This Data Agreement is made in the State of Arizona and shall be interpreted 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.

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

21. Arbitration. To the extent required by A.R.S. §§12-1518 and 12-133, the parties agree to resolve any dispute arising out of this Agreement by arbitration.

22. Amendments. All references to provisions of statutes, codes and regulations include any and all amendments thereto.

23. Miscellaneous. The provisions of this Data Agreement shall survive the termination, cancellation or completion of all work, services, performance 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 the 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.

Vendor Name: Amplify Education, Inc.

By: Richard Morris

Printed Name: Richard Morris

Title: SVP, Finance

Date: 08 / 31 / 2022

Scottsdale Unified School District #48

By: Scott A Menzel

Printed Name: Dr. Scott A. Menzel

Title: Superintendent

Date: 9/12/22 15:54 MST

Exhibit "A"
Security Incident

1. Data Security Incident. If Amplify Education Inc. ("Amplify") has reason to believe that Student Data are disclosed to or acquired by an unauthorized individual(s) (a "Security Incident"), then Amplify will fully investigate the incident and to take reasonable steps to remediate systems and controls and to mitigate any potential harm to individuals which may result from the Security Incident and cooperate with District's investigation of the Security Incident.

2. Notification to District. Amplify will notify District after Amplify determines that District's Student Data were affected by the Security Incident, subject to applicable law and authorization of law enforcement personnel, if applicable. To the extent known, Amplify will identify in such a notification the following: (i) the nature of the Security Incident, (ii) the steps Amplify has executed to investigate the Security Incident, (iii) the type(s) of personally identifiable information that was subject to the unauthorized disclosure or acquisition, (iv) the cause of the Security Incident, if known, (v) the actions Amplify has done or will do to remediate any deleterious effect of the Security Incident, and (vi) the corrective action Amplify has taken or will take to prevent a future Security Incident.

3. Notification to Individuals. To the extent District determines that the Security Incident triggers third party notice requirements under applicable laws, as the owner of the Student Data, the District shall be responsible for the timing and content of the notices to be sent. Except as otherwise required by law, Amplify will not provide notice of the Security Incident directly to individuals whose personal information was affected, to regulatory agencies, or to other entities, without first providing written notice to District. Amplify will be responsible for, and will bear, all notification related costs arising out of or in connection with the Security Incident, subject to any limitations of liability terms contained in the Agreement. For clarity and without limitation, Amplify will not be responsible for costs associated with voluntary notification that is not legally required. With respect to any Security Incident that is not due to acts or omissions of Amplify or its agents, Amplify will reasonably cooperate in performing the activities described above, at District's reasonable request and expense.