3DEZROUTING STUDENT DATA PRIVACY AGREEMENT (2021)

1. DATA OWNERSHIP AND AUTHORIZED ACCESS

1.1 Student Data Property of Local Education Agency (LEA).

All Student Data or any other Pupil Records transmitted to 3DEZROUTING (the Provider) is and will continue to be the property of and under the control of the REED CUSTER CUSD (LEA), or to the party who provided such data (such as the student or parent.).The Provider acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Provider agrees that all rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of The Family Educational Rights and Privacy Act of 1974 (FERPA) and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. The Provider will cooperate and provide Student Data within ten (10) days at the LEA's request. The Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

1.2 Parent Access.

The Provider shall cooperate and respond within ten (10) days to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

1.3 Separate Account.

The Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.

1.4 Third Party Request.

Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact the Provider with a request for data

held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. The Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of the Provider's services.

1.5 No Unauthorized Use.

The Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this agreement (DPA).

2. DUTIES OF THE PROVIDER

2.1 Privacy Compliance.

The Provider shall comply with all Local State and Federal laws and regulations pertaining to data privacy and security.

2.2 Authorized Use.

Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA. The Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.

2.3 Employee Obligation.

The Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. The Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.

2.4 Disposition of Data.

The Provider shall dispose or delete all personally identifiable data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the DPA authorizes the Provider to maintain

personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include: (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. The Provider shall provide written notification to LEA when the Data has been disposed.

2.5 Advertising Prohibition.

The Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or advertising efforts by the Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client.

3. DATA PROVISIONS

3.1 Data Security.

The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of the Provider are set forth below. These measures shall include, but are not limited to:

a) *Passwords and Employee Access.* The Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data. The Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.

b) *Destruction of Data.* The Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. The Provider shall not maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

c) *Security Protocols.* Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. The Provider shall maintain all data obtained or generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA.

d) *Employee Training.* The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, the Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e) *Security Technology*. When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. The Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.
f) *Security Coordinator*. The Provider shall provide the name and contact information of the Provider's Security Coordinator for the Student Data received pursuant to the DPA.
g) *Periodic Risk Assessment*. The Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
h) *Backups*. The Provider agrees to maintain backup copies, backed up at least daily, up to 30 days of Student Data in case of the Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.
i) *Audits*. Upon receipt of a request from the LEA, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof. The Provider will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide full access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider. Failure to cooperate shall be deemed a material breach of the Agreement.

3.2 Data Breach.

In the event that Student Data is accessed or obtained by an unauthorized individual, the Provider shall provide notification to LEA within ten (10) days of the incident. The Provider shall follow the following process:

a) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
b) The security breach notification described above in section 3.2(a) shall include, at a minimum, the following information:
    i. The name and contact information of the reporting LEA subject to this section.
    ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
    iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
    v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c) At LEA's discretion, the security breach notification may also include any of the following:
    i. Information about what the agency has done to protect individuals whose information has been breached.
    ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d) The Provider agrees to adhere to all requirements in the state and federal law respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
e) The Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
f) At the request and with the assistance of the District, the Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

Signature:

REED CUSTER CUSD (LEA)	3DEZROUTING INC (PROVIDER)
	Dale Dorsey
Date: 5/10/2021	Date: 05/10/2021