

**DATA SHARING AGREEMENT BETWEEN
UNION COUNTY BOARD OF EDUCATION
AND
*Requestor***

This Data Sharing Agreement ("DSA") is made by and between Union County Board of Education ("School District"), a local education agency, and *Vendor* ("Requestor") a LEADR. This DSA has the following goals:

- a. Preserve the anonymity of student identities, including assurance that identifiable student data is not released to third parties; and
- b. Enhance the ability of School District and the Requestor to improve academic achievement for School District students by allowing access to individual student records consistent with the requirements of the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. 1232g.

1. Term:

- a. This DSA shall commence on July 1, 2021 and end on June 30, 2022.
- b. *Termination.* This DSA may be terminated by either party hereto upon thirty (30) days written notice.

2. Authorized Representative: For the purposes of the Family Educational Rights and Privacy Act ("FERPA"), the School District designates Requestor an "authorized representative" pursuant to 20 U.S.C. §1232g(b)(1)(C) and 34 C.F.R. §99.31(a)(3). Requestor and the School District shall comply with the provisions of FERPA in all respects. Nothing in this DSA may be construed to allow either party to maintain, use, disclose, or share personally identifiable student information in a manner not allowed by state or federal law or regulation.

3. Definitions:

- a. "Confidential Information" shall include any personally identifiable student information, as that term is defined in 34 C.F.R. §99.3.
- b. "Disclose" or "disclosure" means to permit access to or the release, transfer, or other communication of Confidential Information contained in educational records by any means, including oral, written, or electronic, to any party except the party identified as the party that provided or created the record.

4. Obligations of the School District:

- a. The School District may disclose Confidential Information to Requestor for the purpose of carrying out an audit or evaluation of Federal- or State-supported

education programs, to enforce or comply with Federal legal requirements that relate to those programs described in paragraph 9. Further disclosure by Requestor of any Confidential Information released to Requestor by the School District is prohibited by this DSA and FERPA, 34 C.F.R. Part 99.33.

- b. The types of Confidential Information which may be necessary to disclose to Requestor under this DSA may include the following: Student Name, Student Identifier, Gender, Race/Ethnicity, Grade, IDEA Indicator, Limited English Proficiency Status, Section 504 Status, Title I Targeted Assistance Participation, State, District Number, District Name, School Number, and School Name. No other personally identifiable student information will be disclosed to Requestor unless noted herein: _____.

5. Obligations of Requestor:

- a. Requestor shall not:
 - i. Disclose any Confidential Information to any unauthorized third party, unless such disclosure is required by law or court order;
 - ii. Make any use of Confidential Information except as to perform its obligations under this DSA; or
 - iii. Make any Confidential Information available to any of its employees, officers, or agents except those internal Requestor employees who have been authorized by Requestor to use the information as a component of their project assignment(s).

The term "authorized third party" for the purposes of this DSA does not include employees, officers, or agents of the School District who are authorized to have access to Confidential Information.

- b. Requestor shall use Confidential Information provided by the School District only for the purposes agreed upon by the parties and specified herein.
_____.
- c. Requestor shall protect Confidential Information in such a manner that it will be disclosed only to Requestor staff whose duties under this DSA specifically require them to have access to the Confidential Information.
- d. Requestor shall take reasonable security precautions and protections to ensure that persons not authorized to view the data do not gain access to the data. Reasonable security precautions and protections include, but are not limited to:
 - i. Creating, distributing, and implementing data governance policies and procedures which protect School District data through appropriate administrative, technical, and physical security safeguards and outline staff responsibilities for maintaining data security;
 - ii. Encrypting all School District data carried on mobile computers/devices;

- iii. Encrypting School District data before it is transmitted electronically;
 - iv. Requiring that users be uniquely identified and authenticated before accessing School District data;
 - v. Establishing and enforce well-defined data privilege rights which restrict users' access to the data necessary for them to perform their job functions;
 - vi. Ensuring that all staff accessing School District data sign an affidavit of nondisclosure and maintain copies of signed affidavits;
 - vii. Securing access to any physical areas/electronic devices where sensitive data are stored;
 - viii. Installing a firewall to permit or deny network transmissions based upon a set of rules; and
 - ix. Installing anti-virus software to protect the network.
- e. Upon request of the School District, Requestor shall agree to permit the School District to review or shall provide written assurance to the School District regarding the use of Confidential Information under this DSA. The purpose of this provision is to ensure that appropriate policies and procedures are in place to protect the Confidential Information and that there has been no further Disclosure of Confidential Information.
- f. All Requestor employees, officers, and agents with access to the Confidential Information must acknowledge that they are aware of and will abide by the provisions of this DSA. Requestor agrees to remove any person from performing work who has, or is suspected to have, violated the terms of this DSA.
- g. Requestor understands that the Confidential Information is protected under state and federal law and agrees to notify the School District if any Confidential Information is disclosed, either intentionally or inadvertently, or is suspected to have been disclosed within one hour of discovery.
6. Ownership of Data: By disclosing Confidential Information to Requestor, the School District is in no way assigning ownership to the Confidential Information to Requestor. Upon termination of this DSA for any reason, Requestor shall immediately return all Confidential Information, including all copies, to the School District or destroy all Confidential Information in its possession, custody, or control unless otherwise agreed to in writing by both parties. Requestor will provide School District with affidavits to this effect.
7. Mutual Indemnification:
- a. Requestor agrees to the fullest extent permitted by law, that it will hold harmless, defend, and indemnify the School District, its agents, employees and board members from any liability, cost, or expense, including without limitation penalties, losses, damages, attorneys' fees, taxes, expense of litigation, judgments, liens, and

encumbrances, to the extent arising out of or resulting from any act or omission by Requestor under this DSA. The terms of this section shall survive the termination of this DSA.

- b. School District agrees to the fullest extent permitted by law, that it will hold harmless, defend, and indemnify the Requestor, its agents, employees and board members from any liability, cost, or expense, including without limitation penalties, losses, damages, attorneys' fees, taxes, expense of litigation, judgments, liens, and encumbrances, to the extent arising out of or resulting from any act or omission by School District under this DSA. The terms of this section shall survive the termination of this DSA.

8. Notices: Requestor and the School District shall identify at least one authorized representative or data custodian from their respective agencies who shall be responsible for processing and responding to data requests from the other party.

All notices contemplated or required under the DSA shall be in writing and delivered as follows:

To the District:

Technology Services:

AND

General Counsel:

Michele E. Morris
Union County Public Schools
400 N Church Street
Monroe, NC 29112
704/296-5177

To the Requestor:

9. Miscellaneous:

- a. *Entire Agreement.* This DSA constitutes the entire agreement between the parties and supersedes all prior oral or written agreements, commitments, or understandings concerning the matters provided herein.
- b. *Amendment.* Modification to this DSA must be in writing and signed by each party.
- c. *Governing Law.* This DSA shall be governed by and construed in accordance with the laws of the State of North Carolina. The venue of any lawsuit pertaining to or affecting this DSA shall be in North Carolina.

- d. *Severability.* If any provision of this DSA is held to be invalid or unenforceable, the remainder of the DSA will not be affected, but continue in full force.
- e. *Assignment.* Neither party shall assign its rights or responsibilities under this DSA unless it receives written permission from the other party.
- f. *Non-Waiver.* Any express waiver or failure to exercise promptly any right under this DSA will not create a continuing waiver or expectation of non-enforcement.
- g. *Counterparts.* The parties agree that this DSA may be executed in one or more counterparts, each of which shall constitute an enforceable original of the DSA, and that facsimile signatures shall be as effective and binding as original signatures.

In witness hereto, the parties signify this agreement by signature below:

Superintendent
Union County Public Schools



Recipient Representative

Date

7.14.2021

Date