DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

The Linked Information Network of Colorado
Data Sharing Agreement

1. Preamble

This Data Sharing Agreement ("Agreement"), is by and between School District No. 1 in the City and County of Denver and State of Colorado, d/b/a Denver Public Schools ("Provider") and The Governor's Office of Information Technology, ("OIT"), with its principal place of business at 601 East 18th Avenue, Denver, CO 80203 and is effective as of the last date of signature shown below (the "Effective Date").

WHEREAS, OIT will act as the linking hub of The Linked Information Network of Colorado (LINC).

WHEREAS, Provider wishes to share data with OIT in accordance with the terms and conditions of the Denver Public Schools Data Protection Addendum in Attachment B and the LINC-specific terms and conditions of this Agreement. Data will only be shared with OIT for the purposes of a LINC Project when approved under the terms and conditions of the LINC Enterprise Memorandum of Understanding (EMOU) executed by OIT on July 26, 2019 and the Provider's Joinder Agreement executed by Provider, the validity of which are acknowledged and incorporated herein as Attachment A.

NOW, THEREFORE, the parties, in consideration of mutual promises and obligations set forth herein, the sufficiency of which is hereby acknowledged, and intending to be legally bound, agree as follows:

2. Transfer of Data from Provider to OIT

Provider will submit to OIT, or otherwise permit OIT's LINC staff to electronically access, the data associated with approved LINC Projects in accordance with the LINC EMOU. Confidential Data will be transferred electronically only via encrypted files and in accordance with OIT's data security standards and the State of Colorado's cybersecurity policies (http://www.oit.state.co.us/ois/policies).

3. OIT's Rights to Share/Redistribute the Data

Except as expressly provided in this Agreement and approved by Provider under the terms and conditions of the LINC EMOU, any data submitted to LINC by the Provider will not be further distributed without Provider's written approval.

4. Data Access, Security, Use, and Deletion.

OIT will comply with the following access and security requirements:

a. Limited Access. OIT will limit access to the Confidential Data to LINC Data Integration Staff who have signed the Confidentiality Agreement in Attachment C and are working on a specific LINC Project with the Provider under the terms of the LINC EMOU. OIT will

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

only provide Anonymized Data to LINC Data Recipients of approved LINC Projects as defined in the accompanying LINC EMOU.

b. Secure Storage. The expectations for LINC security storage in OIT are specified in the Denver Public Schools Data Protection Addendum in Attachment B of this Agreement.

c. Use. OIT shall use the Confidential Data solely for purposes approved through the LINC EMOU ("Purpose"). OIT shall only disclose the Confidential Data to LINC Data Integration Staff who have the authority to handle the data in furtherance of the Purpose. OIT will only provide approved LINC Project Data to LINC Data Recipients who have signed the LINC Data Use License in Attachment D.

d. Data Deletion. For approved LINC Projects that require data matching once, OIT shall retain the Provider's Confidential Data for LINC projects for a period of three months after providing the Anonymized Data to the LINC Data Recipient. After this three-month period, all Confidential Data will be deleted by OIT, unless otherwise directed by the Provider in writing to hold the data for an extended time period. For approved LINC Projects requiring multiple data matches over the life of the project, OIT shall retain an encrypted file that contains only the data necessary for matching and the unique LINC identifier. This encrypted identity file will be destroyed three months after the last required data match for the approved LINC Project. OIT shall retain the Anonymized Data related to the approved LINC project for the life of the project period as identified in the Data Use License (DUL) included as Attachment D.

5. Anonymization of LINC Project Data

a. Criteria for Anonymized Data. Only Anonymized Data may be released to LINC Data Recipients for approved LINC Projects. The Provider has determined that Anonymized Data shall remove all direct personal identifiers which can alone be used to distinguish or trace an individual's identity. These include name, birth date, residential address, phone number, state-assigned student identifier, and social security number.

b. Cell Suppression Policy. OIT agrees that LINC Projects including data from the Provider in the creation of any dissemination materials (manuscript, table, chart, study, report, presentation, etc.) must adhere to the cell size suppression policy as follows. This policy stipulates that no cell (e.g., grouping of individuals, patients, clients) with less than 16 observations may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in a cell displaying less than 16 observations. Individual level records may not be published in any form, electronic or printed. Reports and analytics must use complementary cell suppression techniques to ensure that cells with fewer than 16 observations cannot be identified by manipulating data in adjacent rows, columns or other manipulations of any combination of dissemination materials generated through LINC Projects. Examples of such data elements include, but are not limited to, geography, age groupings, sex, or birth or death dates. This cell suppression policy is included in the LINC DUL included as Attachment D.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Provider Responsibilities for Meeting Legal Requirements

Provider has collected the Confidential Data from individuals. Accordingly, Provider is solely responsible for ensuring that all legal requirements have been met to collect data on individuals whose Confidential Data are being provided to LINC.

6. Confidentiality and Breach Notification

a. Confidentiality. All LINC Data Integration Staff shall be informed of the confidentiality obligations imposed by this Agreement and must agree to be bound by such obligations prior to disclosure of Confidential Data to LINC Data Integration Staff, as evidenced by their signature on the Confidentiality Agreement in Attachment A. OIT shall protect the Confidential Data by using the same degree of care as OIT uses to protect its own confidential information, and no less than a reasonable degree of care.

b. Security Incident and Security Breach. The expectations of OIT should a security breach occur are specified in the Denver Public Schools Data Protection Addendum in Attachment B of this Agreement.

7. Modification; Assignment; Entire Agreement

This Agreement may not be modified except by written agreement of the Provider and OIT. This Agreement may not be assigned or transferred without the Provider and OIT's prior written consent. Subject to the foregoing, this Agreement will be binding upon and inure to the benefit of, and be enforceable by, the Provider and OIT and its successors and assigns. Notwithstanding anything to the contrary, each party has the right to disclose the terms and conditions of this Agreement to the extent necessary to establish rights or enforce obligations under this Agreement. This Agreement supersedes all previous LINC Data Sharing Agreements, whether oral or in writing.

8. No Further Obligations

The Provider and OIT do not intend that any agency or partnership relationship be created by this Agreement. No party has any obligation to provide any services using or incorporating the Confidential Data unless the Provider agrees and approves of this obligation under the terms of the LINC EMOU. Nothing in this Agreement obligates the Provider to enter into any further agreement or arrangements relating to disclosure of information or data.

Compliance with Law, Applicable Law

The Provider and OIT agree to comply with all applicable laws and regulations in connection with the Denver Public Schools Data Protection Addendum included as Attachment B to this Agreement. The Provider and OIT agree that this Agreement shall be governed by the laws of the State of Colorado, without application of conflicts of laws principles.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

9. Term of Agreement

The Provider and OIT may terminate this Agreement upon sixty (60) days' written notice to the other party. The terms of this Agreement that by their nature are intended to survive termination will survive any such termination as to Confidential Data provided, and performance of this Agreement, prior to the date of termination, including Sections 2, 3, 4, 5, 6, 7, 8, 9, and 10. The Provider retains the right to terminate this agreement according to the terms specified in the Denver Public Schools Data Protection Addendum included as Attachment B to this Agreement.

10. Use of Name

Neither the Provider nor OIT will use the name of the other party or its employees in any advertisement or press release without the prior written consent of the other party.

11. Definitions

a. Anonymized Data: Data where appropriate personal identifiers have been removed for a LINC Data Recipient such that the likelihood of being able to re-identify individuals is extremely low. The criteria for Anonymized Data are outlined in section 5a.
b. Confidential Data: Data submitted by the Provider that have not been Anonymized.
c. Data Use License (DUL): Agreement between OIT and the LINC Data Recipient that outlines the role and responsibilities of the LINC Data Recipient. The DUL shall include the LINC Project objectives, methodology, data description, data security plan, completion date, reporting requirements, data privacy requirements, and terms for data destruction.
d. LINC Data Integration Staff: The individuals within the Linking Hub who will have the approved responsibility of handling and securing relevant Confidential Data from Parties for approved LINC Projects. The LINC Data Integration Staff will consult with Party staff, clean Confidential Data, link Confidential Data, and prepare Anonymized Data for LINC Projects.
e. LINC Data Recipient: The individual or organization that has received approval for a LINC Project to use integrated Anonymized Data for analysis, research, or evaluation purposes. The LINC Data Recipient may be an employee from a LINC Data Provider or an external researcher.
f. LINC Project: A project approved under the terms of the LINC EMOU. A LINC Project must be analytic, research, or evaluative in nature. A LINC Project must require Confidential Data from two or more Data Providers and must be achievable by LINC Data Recipients with Anonymized Data.

[*Remainder of page left intentionally blank, continue on subsequent page*]

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

12. Representatives

The contacts for purposes of this Agreement are:

For Provider: Jennifer Krause Associate Chief of Impact	For OIT: Alex Pettit Chief Technology Officer

IN WITNESS WHEREOF, the undersigned have executed this Agreement as of the Effective Date.

OIT

By: DocuSigned by: Alex Pettit 2D7A93E9FE054B8...

Name: Alex Pettit
Title: Chief Technology Officer

Date: 1/25/2021

PROVIDER

By: DocuSigned by: Jennifer Krause 4ACE47CC4F014EC...

Name: Jennifer Krause
Title: Associate Chief of Impact

Date: 2/22/2021

APPROVED AS TO FORM:

By: _____
Office of the General Counsel

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Attachment A: [LINC EMOU AND JOINDER AGREEMENT]

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Attachment B:

DATA PROTECTION ADDENDUM

This Data Protection Addendum ("Addendum") is attached to and applies to all services provided by Contractor to District, whether by contract, memorandum of understanding or other form of agreement (the "Contract"), by and between School District No. 1 in the City and County of Denver and State of Colorado, d/b/a Denver Public Schools ("District") and The Colorado Governor's Office of Information Technology ("Contractor") (the Addendum and the Contract are collectively referred to hereinafter as "Agreement"). This Addendum supersedes the Contract by adding to, deleting from and modifying the Contract as set forth herein. To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Contract and this Addendum, this Addendum shall govern and the terms of the Contract that conflict with this Addendum or are inconsistent with this Addendum shall be of no force or effect.

In consideration of the mutual covenants, promises, understandings, releases and payments described in the Contract and this Addendum, the parties agree to amend the Contract by adding the following language:

1. Definitions

1.1. "*Biometric Record*," as used in the definition of "Personally Identifiable Information," means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

1.2. "*Designated Representative*" means District or Contractor employees as specified on Schedule 1 to whom all notices required in this Addendum will be sent.

1.3. "*District Data*" means any Personally Identifiable Information, Record, Education Records, as defined herein, and all Personally Identifiable Information included therein or derived therefrom that is not intentionally made generally available by the District on public websites or publications but is made available directly or indirectly by the District to Contractor or that is otherwise collected or generated by Contractor in connection with the performance of the Services, as defined herein.

1.4. "*De-identified Data*" means District Data from which all Personally Identifiable Information, as defined herein, and attributes about such data, have been permanently removed so that no individual identification can be made.

1.5. "*Education Records*" means records, files, documents and other materials that: (a) contain information directly related to a student; and (b) are maintained by the District, or by a party acting for the District such as Contractor.

1.6. "*End User*" means individuals authorized by the District to access and use the Services as defined herein.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

1.7. "*Incident*" means a suspected, attempted, or imminent threat of unauthorized access, use, disclosure, breach, modification, disruption or destruction to or of District Data.

1.8. "*Mine District Data*" means the act of searching through, analyzing, accessing, or extracting District Data, metadata, or information not necessary to accomplish the Services or purpose(s) of this Agreement for the benefit of the District.

1.9. "*Personally Identifiable Information*" or "*PII*" means information and metadata that, alone or in combination, is linked or linkable to a specific student so as to allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Personally Identifiable Information includes, but is not limited to: (a) the student's name; (b) the name of the student's parent or other family members; (c) the address or phone number of the student or student's family; (d) personal identifiers such as the student's state-assigned student identifier, social security number, student number or biometric record; (e) indirect identifiers such as the student's date of birth, place of birth or mother's maiden name; and (f) demographic attributes, such as race, socioeconomic information, and gender.

To the extent it is not already included in the definition hereinabove, PII also includes: (a) "personal information" as defined in the Colorado Open Records Act, C.R.S. 24-72-101 et seq. ("CORA"); (b) Personally Identifiable Information contained in student "education records" as that term is defined in the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; (c) "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) "nonpublic personal information" as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (e) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; and (f) other financial account numbers, access codes, and state- or federal-identification numbers such as driver's license, passport or visa numbers.

1.10. "*Record*" means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

1.11. 1.10 "*Securely Destroy*" means to remove District Data from Contractor's systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in National Institute of Standards and Technology ("NIST") SP 800-88 r1 (2014) or as amended Guidelines for Media Sanitization so that District Data is permanently irretrievable in Contractor's and its Subcontractors' normal course of business.

1.12. "*Security Breach*" means an event in which District Data is exposed to unauthorized disclosure, access, alteration or use or a system configuration that results in

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

a documented unsecured disclosure, access, alteration or use, in a manner not permitted in this Addendum, which poses a significant risk of financial, reputational or other harm to the affected End User or the District.

1.13. "*Services*" means any goods or services acquired by the District from the Contractor, or under the contract, including but not limited to computer software, mobile applications (apps), and web-based tools accessed by End Users through the Internet, installed, or run on a computer or electronic device.

1.14. "*Subcontractor*" means Contractor's employees, subcontractors or agents, identified on Schedule 2, as updated by Contractor from time to time in accordance with the requirements of this Addendum, who Contractor has engaged to enable Contractor to perform its obligations under the Contract.

1.15. "*Student Profile*" means a collection of PII data elements relating to a student of the District.

2. Rights and License in and to District Data

District owns all rights, title, and interest in and to District Data and any and all now known or hereafter existing intellectual property rights associated therewith, and any derivative works thereof or modifications thereto, including without limitation, De-identified Data. The District hereby grants to Contractor a limited, nonexclusive license to use District Data solely for the purpose of performing its obligations specified in the Contract. This Agreement does not give Contractor any rights, title, or interest implied or otherwise, to District Data or De-identified Data, except as expressly stated in the Contract.

3. Data Privacy

3.1 Use of District Data. Contractor shall use District Data only for the purpose of performing the Services and fulfilling its duties under the Contract.

3.2 Prohibited Uses of District Data. With the exception of De-identified Data that the District has agreed in writing to allow Contractor to use as specified in Section 3.5, Contractor shall not:

3.2.1 Use, sell, rent, transfer, distribute, alter, mine, or disclose District Data (including metadata) to any third party without the prior written consent of the District, except as required by law;

3.2.2 Use District Data for its own commercial benefit, including but not limited to, advertising or marketing of any kind directed toward children, parents, guardians, or District employees, unless such use is specifically authorized by this Agreement or otherwise authorized in writing by the District;

3.2.3 Use District Data in a manner that is inconsistent with Contractor's privacy policy;

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

3.2.4 Use District Data to create a Student Profile other than as authorized or required by the Contract to perform the Services; and

3.2.5 Store District Data outside the continental United States unless Contractor has given the District Designated Representative advance written notice of where and how the servers are housed, managed, and secured, and that the security standards required herein can be achieved.

3.3 Qualified FERPA Exception. If Contractor will have access to Education Records, Contractor acknowledges that, for the purposes of this Agreement, pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA"), it will be designated as a "school official" with "legitimate educational interests" in the District Education Records and PII disclosed pursuant to the Contract, and Contractor agrees to abide by the FERPA limitations and requirements imposed on school officials. Contractor will use the Education Records only for the purpose of fulfilling its duties under the Contract for District's and its End Users' benefit, and shall not share District Data with or disclose it to any third party except as provided for in the Agreement, as required by law, or if authorized in writing by the District. Contractor warrants and represents that during the five-year period preceding the Effective Date of this Agreement, it has not been found in violation of FERPA by the U.S. Department of Education's Family Policy Compliance Office.

3.4 Subcontractor Use of District Data. To the extent necessary to perform its obligations specified in the Contract, Contractor may disclose District Data to Subcontractors pursuant to a written agreement, specifying the purpose of the disclosure and providing that: (a) Subcontractor shall not disclose District Data, in whole or in part, to any other party; (b) Subcontractor shall not use any District Data to advertise or market to students or their parents/guardians; (c) Subcontractor shall access, view, collect, generate and use District Data only to the extent necessary to assist Contractor in performing its obligations specified in the Contract; (d) at the conclusion of its/their work under its/their subcontract(s) Subcontractor shall, as directed by the District through Contractor, Securely Destroy all District Data in its/their possession, custody or control, or return such District Data to the District, at the election of the District; (e) Subcontractor shall indemnify the District in accordance with the terms set forth in Section 10 hereinbelow; and (f) Subcontractor shall utilize appropriate administrative, physical and technical safeguards in accordance with industry standards and best practices to secure District Data from unauthorized disclosure, access and use. Contractor shall ensure that its employees and Subcontractors who have potential access to District Data have undergone appropriate background screening, to the District's satisfaction, and possess all needed qualifications to comply with the terms of this Addendum. Contractor shall also ensure that its Subcontractors comply with the insurance requirements specified in Section 12 of this Addendum.

3.5 Use of De-identified Data. Contractor may use De-identified Data for purposes of research, the improvement of Contractor's products and services, and/or the development of new products and services. In no event shall Contractor or Subcontractors re-identify or attempt to re-identify any De-identified Data or use De-identified Data in combination with other data elements

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

or De-identified Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

3.6 Privacy Policy Changes. Prior to making a material change to Contractor's privacy policies, Contractor shall send District's Designated Representative written notice, which includes a clear explanation of the proposed changes.

4. Data Security

4.1 Security Safeguards. Contractor shall store and process District Data in accordance with commercial best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in SANS Top 20 Security Controls, as amended, to secure such data from unauthorized access, disclosure, alteration, and use. Contractor shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with all applicable federal and state data protection and privacy laws, regulations and directives, including without limitation C.R.S. § 22-16-101 *et seq.*, as well as the terms and conditions of this Addendum. Without limiting the foregoing, and unless expressly agreed to the contrary in writing, Contractor warrants that all electronic District Data will be encrypted in transmission and at rest in accordance with NIST Special Publication 800-57, as amended.

4.2 Risk Assessments. Contractor shall conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

4.3 Audit Trails. Contractor shall take reasonable measures, including audit trails, to protect District Data against deterioration or degradation of data quality and authenticity, and to ensure data is deidentified in accordance with this Addendum.

4.4 Verification of Safeguards. Upon District's written request, Contractor shall provide or make available to the District for review, one or more of the following, verifying Contractor's administrative, physical and technical safeguards are in compliance with industry standards and best practices: (1) a third-party network security audit report; (2) certification from Contractor indicating that an independent vulnerability or risk assessment of the Contractor's data security program has occurred; (3) district data has been deidentified by Contractor as set forth in the definition of Deidentified Data in section 1.3 of this Addendum.

4.5 Background Checks. The Contractor and every person, including any subcontractor or agent of the Contractor, who provides direct services to students, or who has access to student data, shall be required to have a criminal background check that meets the requirements of § 22-32-109.7, C.R.S. and other District requirements, including a fingerprint-based conviction investigation. Conducting a Colorado Bureau of Investigation criminal history check or a Name Check investigation for any person providing services under this Contract does not meet District requirements. The costs associated with the background checks are solely the Contractor's responsibility. Thereafter, any personnel, subcontractor, volunteer or agent hired or added during the term of this Contract shall satisfy the requirements set forth in this Section before performing services on Contractor's behalf. The Contractor shall make the background check results available

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

upon request of the District in compliance with the provisions of § 24-72-305.3, C.R.S. The District also reserves the right to conduct its own criminal background check of every person before Services begin.

4.5.1 Notwithstanding the criminal background check requirement as set forth above, Contractor hereby certifies that no employee, subcontractor, volunteer or agent of the Contractor performing the Services has been convicted in Colorado or in any other State of a criminal offense involving: (i) the abuse, abduction, sexual molestation, physical or sexual assault on, or rape of a minor; or (ii) any crime involving exploitation of minors, including but not limited to, child pornography offenses or any crime of violence. Contractor shall notify the District immediately upon the discovery or receipt of any information that any person performing services on Contractor's behalf has been detained or arrested by a law enforcement agency of the aforementioned crimes. Contractor understands that allowing any employee, subcontractor, volunteer or agent of the Contractor performing the Services who has been arrested or convicted of the aforementioned crimes to: (i) provide direct services to students, (ii) access student data, or (iii) enter onto District property, constitutes a material breach of this Contract and may result in the immediate termination of this Contract and referral to law enforcement for possible criminal charges, or additional civil sanctions pursuant to federal and state law. Misdemeanor conviction(s) may not necessarily result in the immediate termination of this Contract. Misdemeanor convictions are evaluated on a case-by-case basis, considering the nature and gravity of the offense, time elapsed since the offense, conviction, or time served, and the nature of the Services. Upon the District's request, Contractor shall provide documentation of every person performing the Services to substantiate the basis for this certification.

5. Security Incident and Security Breach

5.1 Security Incident Evaluation. In the event of an Incident, Contractor shall follow industry best practices to fully investigate and resolve the Incident, and take steps to prevent developments that may result in the Incident becoming a Security Breach at Contractor's expense in accordance with applicable privacy laws.

5.2 Response. Immediately upon becoming aware of a Security Breach, or a complaint of a Security Breach, Contractor shall notify the District Designated Representative in writing as set forth herein, fully investigate the Security Breach, cooperate fully with the District's investigation of and response to the Security Breach, and use best efforts to prevent any further Security Breach at Contractor's expense in accordance with applicable privacy laws. Except as otherwise required by law, Contractor shall not provide notice of the Security Breach directly to individuals whose Personally Identifiable Information was involved, to regulatory agencies, or to other entities, without first providing written notice to the District's Designated Representative.

5.3 Security Breach Report. If the District reasonably determines that Contractor has committed a Security Breach, then the District may request Contractor to submit, within seven (7) calendar days from discovery of such breach, a written report, and any supporting documentation, identifying (i) the nature of the Security Breach, (ii) the steps Contractor has executed to investigate the Security Breach, (iii) what District Data or PII was used or disclosed, (iv) who or what was the cause of the Security Breach, (v) what Contractor has done or shall do to remediate

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

any deleterious effect of the Security Breach, and (vi) what corrective action Contractor has taken or shall take to prevent a future Incident or Security Breach. The District reserves the right to require Contractor to amend its remediation plans.

5.4 Effect of Security Breach. Upon the occurrence of a Security Breach, the District may terminate this Agreement in accordance with District policies. The District may require Contractor to suspend all Services, pending the investigation and successful resolution of any Security Breach, and Contractor may be required to reimburse District all amounts paid for any period during which Services were not rendered. Contractor acknowledges that, as a result of a Security Breach, the District may also elect to disqualify Contractor and any of its Subcontractors from future contracts with the District.

5.5 Liability for Security Breach. In addition to any other remedies available to the District under law or equity, Contractor shall reimburse the District in full for all costs, including but not limited to, payment of legal fees, audit costs, fines, and other fees imposed that were actually incurred by the District and caused in whole or in part by Contractor or Contractor's Subcontractors for any Security Breach. If Personally Identifiable Information is compromised, Contractor shall provide notification to the affected individuals on behalf of the District, pursuant to the Student Data Transparency and Security Act, C.R.S. 22-16-108 (4). Contractor shall provide one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during any Security Breach could be used to commit financial identity theft.

6. Response to Legal Orders, Demands or Requests for Data

6.1 Received by Contractor. Except as otherwise expressly prohibited by law, Contractor shall immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking District Data; consult with the District regarding its response; cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and, upon the District's request, provide the District with a copy of its response.

6.2 Received by District. If the District receives a subpoena, warrant, or other legal order, demand or request seeking District Data maintained by Contractor, including but not limited to, a request pursuant to the CORA, the District will promptly notify Contractor and, within two (2) business days, excluding national holidays, Contractor shall supply the District with copies of the District Data for the District to respond.

6.3 Parent Request. If a parent, legal guardian or student contacts the District with a request to review or correct District Data or PII, pursuant to FERPA or the Student Data Transparency and Security Act, C.R.S. § 22-16-101 *et seq.* (the "Act"), the District will promptly notify Contractor's Designated Representative and Contractor shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District, within ten calendar (10) days after receipt of District's notice. Conversely, if a parent, legal guardian or student contacts the Contractor with a request to review or correct District Data or PII, within ten calendar (10) days after receipt of such notice, Contractor shall promptly notify the District and

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District.

6.4 Access to District Data. District shall have the right to access and retrieve any or all District Data stored by or in possession of Contractor upon written notice to Contractor's Designated Representative. Contractor shall make the District Data available to the District within seven (7) calendar days from the date of request.

7. Compliance with Applicable Law

7.1. Children's Online Privacy and Protection Act. If Contractor collects personal information (as defined in the Children's Online Privacy and Protection Act of 1998, 5 U.S.C. 6501 to 6505, and its implementing regulations ("COPPA")) from children under thirteen (13) years of age in performing the Services, Contractor warrants, represents, and covenants that such collection is and shall be for the use and benefit of the District and for no other commercial purpose. Contractor has provided District with written notice of its collection, use, and disclosure practices.

7.2 Compliance with Laws. Contractor warrants that it will abide by all applicable laws, ordinances, rules, regulations, and orders of all governmental agencies or authorities having jurisdiction over the Services including but not limited to: (a) COPPA; (b) FERPA; (c) the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) the Health Information Technology for Economic and Clinical Health Act, (e) Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (f) Payment Card Industry Data Security Standards; (g) Protection of Pupil Rights Amendment, 20 U.S.C. 1232h, 34 C.F.R. Part 98; and (h) Americans with Disabilities Act, and Federal Export Administration Regulations.

7.3 Americans with Disabilities Act. To the extent the District is required to provide accommodations in compliance with the Americans with Disability Act ("ADA"), Contractor will make best efforts to assist the District in providing its services to end users pursuant to this Agreement, and will assistance the District in a manner that its system and services will, at a minimum, conform with all laws, regulations and guidance that apply to accessibility in accordance with the ADA, Section 504 of the Rehabilitation Act of 1973, and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA guidelines; provided, however, Contractor will have no obligations with respect to such compliance as it relates to any portion of the system and services provided or developed by the District including District content.

8. Term and Termination

8.1 This Addendum takes effect immediately as of the Effective Date, and remains in full force and effect until the successful completion of the services, unless earlier terminated under Sections 8.2 or 12.3.

8.2 Subject to Sections 8.2 and 12.3, this Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Contract between the Parties or successful completion of the Services. Alternatively, upon re-execution of the

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Contract by the authorized persons of District and Contractor, this Addendum shall also be revived and be of full force and effect.

8.2 Termination by the District.

8.2.1 The District may immediately terminate the Contract in accordance with District policies if, at any time, the District determines in its sole discretion, that Contractor has breached any of the requirements of this Addendum.

8.2.2 The District may terminate the Contract if District receives information that Contractor has failed to comply with the same or substantially similar security obligations as set forth herein with another school district.

8.2.3 The District may terminate the Contract if the District receives information after execution of this Addendum, that any of Contractor's representations or warranties have substantially changed after execution of this Addendum, including but not limited to the terms of Contractor's privacy policy.

9. Data Transfer Upon Termination or Expiration

9.1 Destruction or Return of District Data. With the exception of De-identified Data that District has specifically agreed in writing to allow Contractor to use after termination or expiration of this Agreement, or District Data for which Contractor has specifically obtained consent from the parent, legal guardian or student to keep, no later than (30) calendar days after termination or expiration of this Agreement, Contractor shall certify in writing that all District Data and PII that Contractor collected, generated or inferred pursuant to the Contract ("Contract Data"), is securely returned or Securely Destroyed, pursuant to Schedule 4 attached hereto.

9.2 Transfer and Destruction of District Data. If the District elects to have all District Data or Contract Data that is in Contractor's possession or in the possession of Contractor's Subcontractors transferred to a third party designated by the District, such transfer shall occur within a reasonable period of time but no later than thirty (30) calendar days after expiration or termination of this Agreement, and without significant interruption in service or access to such District Data. Contractor shall work closely with such third party transferee to ensure that such transfer/migration uses facilities and methods compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. District will pay all costs associated with such transfer, unless such transfer is as the result of termination of this Agreement following Contractor's breach of the terms of this Agreement. Upon successful transfer of District Data, as confirmed in writing by the District's Designated Representative, Contractor shall Securely Destroy all District Data in accordance with Section 9.1.

9.3 Response to Specific Data Destruction or Return Requests. After receiving a written request from the District, Contractor shall Securely Destroy or return any specific District Data or Contract Data that is in its possession or in the possession of its Subcontractors within five (5) business days, excluding national holidays, after receiving a written request from the District.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

10. Indemnification

10.1 If Contractor is a "public entity" then it will be responsible for the negligent acts and omissions of its officers, agents, employees and representatives with respect to its obligations under this Agreement. Any provision of this Agreement, whether or not incorporated herein by reference, shall be controlled, limited and otherwise modified so as to limit any liability of the Contractor under the Colorado Governmental Immunity Act, C.R.S. 24-10-101 et seq. It is specifically understood and agreed that nothing contained in this paragraph or elsewhere in this Agreement shall be construed as an express or implied waiver of its governmental immunity or as an express or implied acceptance of liabilities arising as a result of actions which lie in tort or could lie in tort in excess of the liabilities allowable under the Act, as a pledge of the full faith and credit of the Partner, or as the assumption by the Partner of a debt, contract or liability of the District or its affiliates in violation of Article Xl, Section 1 of the Constitution of the State of Colorado.

10.2 If Contractor is not a "public entity" then Contractor shall indemnify, defend and hold District and its elected officials, employees, representatives, and agents harmless, without limitation, from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses, including attorneys' fees, the costs of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from Contractor's, or Contractor's subcontractors, performance of services under this Addendum, any third-party claim against any Indemnified party to the extent arising out of or resulting from Contractor's, or Contractor's subcontractors, failure to comply with any of its obligations under Sections 3, 4, 5, and 9 of this Addendum, and any breach of Contractor's, or Contractor's subcontractors, obligations under this Addendum. These indemnification duties shall survive termination or expiration of this Agreement.

11. Insurance

11.1 Coverage. As required by Schedule 5.

12. Miscellaneous

12.1 No Contractor End User Agreements. Contractor shall not require End Users to sign or complete any end user license agreements (EULA) or acceptable use policy (AUP) agreements or understandings, whether electronic, verbal, or in writing. In the event that an EULA or AUP is completed by a District End User, this Addendum shall supersede the Contractor's agreement.

12.2 Public Inspection of Agreement. Contractor acknowledges and agrees that this Agreement and all documents Contractor provides District as required herein, are public records for purposes of the CORA and shall at all times be subject to public inspection. The parties understand that in the event of a request for disclosure of such information, the District will notify Contractor to give Contractor the opportunity to redact its proprietary or confidential material. In the event of the filing of a lawsuit to compel disclosure, the District will tender Contractor's material to the court for judicial determination of the issue of disclosure and Contractor agrees to

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

intervene in such lawsuit to protect and assert its claims of privilege against disclosure or waive the same.

12.3 Survival. The Contractor's obligations under Sections 3, 4, 5, 6, 9, and 10, and any other obligations or restrictions that expressly or by their nature are to continue after termination, shall survive termination of this Agreement for any reason until all District Data has been returned or Securely Destroyed.

12.4 Choice of Law. Any claim, controversy or dispute arising under or related to this Addendum shall be construed pursuant to the substantive, not conflicts, laws of the State of Colorado. Each of the Parties submits to the exclusive jurisdiction of any state court sitting in or federal court with jurisdiction over Denver County, Colorado, in any action or proceeding arising out of or relating to this Agreement and agrees that all claims in respect of the action or proceeding may be heard and determined in any such court. Each Party also agrees not to bring any action or proceeding arising out of or relating to this Addendum in any other court. Each of the Parties waives any defense of inconvenient forum to the maintenance of any action or proceeding so brought and waives any bond, surety or other security that might be required of any other Party with respect to any such action or proceeding.

12.5 Immunities. The District retains all of its rights, privileges and immunities under the Colorado Governmental Immunity Act, C.R.S. § 24-10-101 *et seq*.

12.6 No Assignment. Contractor shall not assign or subcontract any of its rights or obligations hereunder without the express written consent of District. Any assignment in violation of this section shall be void.

12.7 No Third Party Beneficiaries. Nothing in this Agreement shall be construed to give any rights or benefits to anyone other than District.

12.8 Schedules. The following schedules are attached hereto, or shall be attached hereto, and are specifically made a part hereof by this reference:

Schedule 1 – Designated Representatives
Schedule 2 – Subcontractors
Schedule 3 – Written Consent to Maintain De-identified Data
Schedule 4 – Certification of Destruction\Return of District Data
Schedule 5 – Data Elements
Schedule 6 – Insurance

12.9 Counterparts. This Addendum may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

12.10 Effectiveness; Date. This Addendum will become effective when all parties have signed it. The date of this Addendum will be the date this Addendum is signed by the last party to sign it (as indicated by the date associated with the party's signature).

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

12.11 Electronic Signatures and Electronic Records. The Contractor consents to the use of electronic signatures by the District. This Addendum, and any other documents requiring a signature under this Addendum, may be signed electronically by the District in the manner specified by the District. The parties agree not to deny the legal effect or enforceability of this Addendum solely because it is in electronic form or because an electronic record was used in its formation. The parties agree not to object to the admissibility of the Addendum in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party is signing this agreement on the date stated opposite that party's signature.

SCHOOL DISTRICT NO. 1 IN THE CITY AND COUNTY OF DENVER AND STATE OF COLORADO, D/B/A DENVER PUBLIC SCHOOLS

Date: 2/22/2021

By: DocuSigned by: Staci Crum 053FA246B634437...

Staci Crum/DeeDee Case
Manager, Strategic Sourcing

COLORADO GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

Date: 1/25/2021

By: DocuSigned by: Alex Pettit 2D7A93E9EE054B8...

Alex Pettit
Chief Technology Officer

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

SCHEDULE 1
Designated Representatives

DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Name: **Jennifer Collins** **Title:** **Deputy General Counsel** **Address:** **1860 Lincoln St** **Denver, CO 80203** **Phone:** **720-423-2211** **E-mail:** **legal_contracts@dpsk12.org**	**Name:** **Alex Pettit** **Title:** **Chief Technology Officer** **Address:** **601 E 18th Ave #130** **Denver CO 80203** **Phone:** **303-764-7700** **E-mail:** **alex.pettit@state.co.us**

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

SCHEDULE 2
Subcontractors

Contractor shall update this information as necessary to maintain accuracy and shall send revised attachments, exhibits or schedules to the District's Authorized Representative.

What third party vendors does Contractor do business with that may have access to student personally identifiable data, and what is the purpose of these third party vendors (please fill complete the table below with this information)?

Name of Subcontractor	Primary Contact Person	Subcontractor's Address	Subcontractor's Phone/email	Purpose of re-disclosure to Subcontractor
N/A				

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

SCHEDULE 3
Written Consent to Maintain De-identified Data

The District hereby gives its consent for Contractor to retain and use for the stated purpose and period, De-identified Data elements as set forth below:

Description of De-identified Data Elements	**Purpose for Retention and Use**	**Period of Use**
Data approved by District for Linked Information Network of Colorado (LINC) Projects	Research and analytic LINC projects approved by District. Data are held by authorized LINC staff at the Governor's Office of Information Technology and the approved LINC data requestor.	From LINC project start date to project end date specified in LINC Project request

I\We, Alex Pettit, as [title] Chief Technology Officer and the authorized representative(s) of the Contractor do hereby certify that no attempt will be made to re-identify De-identified Data.

Contractor Name: Colorado Governor's Office of Information Technology

Contractor Representative Name: Alex Pettit

Title: Chief Technology Officer

Signature: DocuSigned by: Alex Pettit 2D7A93E9FE054B8... Date: 1/25/2021

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

SCHEDULE 4
Certification of Destruction\Return of District Data

I\We, _____, as the authorized representative(s) of the Contractor do hereby acknowledge and certify under penalty of perjury that [initial next to both subparts of the applicable Part A or Part B]:

Part A - Destruction:

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was destroyed on _____, 20___ by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was destroyed as set forth below:

Name of Subcontractor	*Date of Deletion*	*Destruction Method*

Part B - Return: [If this option is elected by the District, then Contractor shall also complete Part A.]

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District, on _____, 20___ to _____, by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District as set forth below:

Name of Subcontractor	*Date of Return*	*Return / Transfer Method*

Contractor Name: _____

Contractor Representative Name: _____

Title: _____

Signature: _____ Date: _____

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

SCHEDULE 5
Data Elements

(Mandatory to be completed if Service Provider is a School Service Contract Provider under CRS 22-16-101 et seq.)

1. **Service Provider collects, generates or uses pursuant to the Agreement the following data elements of District Data or PII**:

Specific data elements will be determined for each LINC project approved by District representatives. Contractor will not receive any District data until a LINC project request is approved by the District representatives. The LINC project request will include the specific data elements required for the project to be completed.

2. **Service Provider collects and uses the District Data for the following educational purposes**:

LINC performs identity resolution and anonymization for LINC projects approved by District representatives. All LINC projects are for research purposes.

3. **Service Provider's policies regarding retention and disposal of District Data are as follows**:

Contractor will destroy all District data for approved LINC projects 3 months after the end of the LINC project is completed. Contractor will sign a certificate of destruction and will submit to the District for each LINC project.

4. **Service Provider uses, shares or discloses the District Data in the following manner:**

The Contractor will only share anonymized approved LINC project data with requesters. No direct PII will ever be shared by the Contractor.

5. **Has Service Provider's agreement has ever been terminated by another school district for failure to comply with the same or substantially similar security obligations as those set forth in this Agreement**?

☐ Yes X No.

If yes, describe:

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

SCHEDULE 6
Insurance

Denver Public Schools

ENTERPRISE RISK MANAGEMENT

Tel: 720-423-1300

General Provisions

Contractor agrees to secure, at or before the time of execution of this Agreement, the following insurance covering all operations, goods or services provided pursuant to this Agreement.

Contractor shall provide a copy of this Agreement to its insurance agent or broker. Contractor may not commence services or work relating to the Agreement prior to placement of coverage.

Contractor shall keep the required insurance coverage in force at all times during the term of the Agreement, or any extension thereof.

Insurer Ratings: The required insurance shall be underwritten by an insurer licensed or authorized to do business in Colorado and rated by A.M. Best Company as "A-" VIII or better.

Cancellation, Non-Renewal Notifications: Each policy shall contain a valid provision or endorsement requiring notification to the District in the event any of the required policies are to be cancelled or non-renewed before the expiration date thereof. Such written notice shall be sent to the parties identified in the Notices section of this Agreement. Said notice shall be sent thirty (30) days prior to such cancellation or non-renewal unless due to non-payment of premiums for which notice shall be sent ten (10) days prior. If such written notice is unavailable from the insurer, Contractor shall provide written notice of cancellation, non-renewal or reduction in limits to the parties identified in the Notices section by certified mail, return receipt requested within three (3) business days of such notice by its insurer(s).

Deductibles or Self-Insured Retentions: If any policy is in excess of a deductible or self-insured retention, the Contractor must notify the District. Contractor shall be responsible for the payment of any deductible or self-insured retention.

Minimum Requirements: The insurance coverages specified in this Agreement are the minimum requirements, and these requirements do not lessen or limit the liability of the Contractor. The Contractor shall maintain, at its own expense, any additional kinds or amounts of insurance that it may deem necessary to cover its obligations and liabilities under this Agreement.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Contractor shall advise the District in the event any general aggregate or other aggregate limits are reduced below the required per occurrence limits. At its own expense, and where such general aggregate or other aggregate limits have been reduced below the required per occurrence limits, the Contractor will procure such per occurrence limits and furnish a new certificate of insurance showing such coverage is in force.

Proof of Insurance: Contractor certifies that any certificate of insurance, (preferably an ACORD certificate), provided as evidence of insurance coverage under this Agreement, complies with all insurance requirements in this Agreement. The District's acceptance of a certificate of insurance or other proof of insurance that does not comply with all insurance requirements set forth in this Agreement shall not act as a waiver of Contractor's breach of this Agreement or of any of the District's rights or remedies under this Agreement. The District's Risk Management Department may require additional proof of insurance including but not limited to policies and endorsements.

Subcontractors and Subconsultants: All Subcontractors and Subconsultants (including Independent Contractors, Suppliers or other entities providing goods or services required by this Agreement) shall be subject to all of the requirements herein and shall procure and maintain the same coverages required of the Contractor. Contractor shall include all such Subcontractors as Additional Insureds under its policies (with the exception of Workers' Compensation) or shall ensure that all such Subcontractors and Subconsultants maintain the required coverages.

Insurance Coverage and Limits

Workers' Compensation/Employer's Liability: Contractor shall maintain the coverage as required by statute and shall maintain Employer's Liability insurance with limits of at least $100,000 per occurrence for each bodily injury claim, $100,000 per occurrence for each bodily injury caused by disease claim, and $500,000 aggregate for all bodily injuries caused by disease claims.

Contractor expressly represents to the District, as a material representation upon which the District is relying on entering into this Agreement, that none of the Contractor's officers or employees who may be eligible under any statute or law to reject Workers' Compensation insurance shall affect such rejection during any part of the term of this Agreement, and that any such rejections previously effected, have been revoked as of the date Contractor executes this Agreement.

Business Automobile Liability: Contractor shall maintain Business Automobile Liability coverage with limits of at least $1,000,000 combined single limit applicable to all owned, hired and non-owned vehicles used in performing services under this Agreement.

Commercial General Liability: Contractor shall maintain Commercial General Liability coverage with limits of at least $1,000,000 for each occurrence, $1,000,000 for each personal and advertising injury claim, $2,000,000 products and completed operations aggregate, and $2,000,000 policy aggregate.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Excess/Umbrella Liability: Contractor shall maintain Excess or Umbrella Liability coverage with limits of at least $1,000,000 per occurrence and $1,000,000 policy aggregate. Coverage must be written on a "follow form" or broader basis.

The following three types of required insurance coverages may be met with separate policies or a combination of these coverages under one policy. If in a combined policy, the combined policy form shall include minimum limits of at least $3,000,000 each occurrence and in the aggregate.

Technology Errors & Omissions: Contractor shall maintain Technology Errors and Omissions Liability coverage including, but not limited, to Network Security, Privacy Liability and Product Failure coverage with limits of at least $1,000,000 per occurrence and $1,000,000 policy aggregate.

Media Professional Liability: Contractor shall maintain Media Professional Liability limits of at least $1,000,000 per claim and $1,000,000 in the aggregate. The policy shall include, but not be limited to, coverage for libel, slander, infringement of copyright, invasion of the right of privacy, and unauthorized use of titles, formats, ideas, characters, plots or other material used in the publication or design.

Cyber/Network Security & Privacy Liability: Contractor shall maintain Cyber/Network Security & Privacy Liability coverage with limits of at least $1,000,000 per occurrence and $1,000,000 policy aggregate including, but not limited to, coverage for claims involving privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security.

Other Insurance Provisions

Additional Insured Status: For Commercial General Liability, Auto Liability, Excess/Umbrella Liability, Cyber/Network Security and Privacy Liability (if applicable), Contractor and Subcontractor's insurer(s) shall name School District No. 1 in the City and County of Denver, d/b/a Denver Public Schools, and its elected officials, employees, representatives and agents as Additional Insureds.

Waiver of Subrogation: For coverages required under this Agreement, Contractor's insurer shall waive subrogation rights against the District.

Primary Coverage: For claims related to this Agreement, Contractor's insurance coverage shall be primary and non-contributory with other coverage or self-insurance maintained by the District.

Claims Made Policies: For claims-made coverage, the retroactive date must be on or before the contract date or the first date when any goods or services were provided to the District, whichever is earlier.

Additional Provisions: Defense costs must be outside the limits of liability. Policies must contain a severability of interests or separation of insureds provision (no insured versus insured exclusion). The Commercial General Liability coverage must provide that this is an Insured Contract under the policy.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Attachment C:

COLORADO GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY
CONFIDENTIALITY AGREEMENT

I, _____, hereby acknowledge that, with regard to a request for information through the Linked Information Network of Colorado (LINC) and the associated Data Sharing Agreement ("Agreement") between the Colorado Governor's Office of Information Technology (OIT) and School District No. 1 in the City and County of Denver and State of Colorado, d/b/a Denver Public Schools (Provider), I may acquire or have access to confidential information or personally identifiable information associated with Colorado residents.

I agree to comply with all the terms of the Agreement regarding the access, use, and disclosure of any information submitted by Provider to OIT.

At all times I will maintain the confidentiality of the information. I will not inspect or "browse" the information for any purpose not identified in the Agreement. I will not access, or attempt to access, my own information, or information relating to an individual or entity with which I have a personal or financial interest, for any reason not necessary to the performance of the work assigned to me under the Agreement. This includes, but is not limited to, information relating to family members, neighbors, relatives, friends, ex-spouses, their employers, and/or anyone not necessary for the work assigned.

At no time will I either directly or indirectly, disclose, or otherwise make the information available to any unauthorized person.

I agree to comply with all applicable state and federal laws and regulations with regard to confidentiality and security of the information, including but not limited to, the following.

Colorado Rules Volume 6 - Section 6.210
Colorado Information Security Act (C.R.S. 24-37.5)
Colorado Revised Statutes Title 26, Article 1, section 26-1-114
Governor's Office of Information Technology, System Applications Statement of Compliance (as revised)
Social Security Act (Title 42 U.S.C)
Privacy Act of 1974
Federal Information Security Management Act of 2002 (FISMA)
Internal Revenue Code Section 6103
Health Insurance Portability and Accountability Act (45 CFR Part 160 and Part 164)
42 Code of Federal Regulations ("CFR") Part 2
The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g and 34 CFR Part 99)

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Civil and criminal penalties for willful misuse of information can be found in the aforementioned citations.

Executed:

_____ _____

Signature Date

Printed Name:

_____

Organization Name:

_____

Telephone: _____ Email: _____

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Attachment D:

The Linked Information Network of Colorado
Data Use License

1. Preamble

This Data Use License ("DUL") is entered as of _____ (the "Effective Date") by _____ ("LINC Data Recipient").

This DUL addresses the conditions under which the Colorado Governor's Office of Information Technology (" OIT") will disclose, and the LINC Data Recipient may use, the Anonymized Data for LINC Projects specified in this DUL and/or any derivative file(s) (collectively, the "LINC Project Data"). The terms of this DUL are consistent with those in the LINC Enterprise Memorandum of Understanding (EMOU) and can be changed only by a written and signed amendment to this DUL or by terminating this DUL and entering a new DUL, after approval by the LINC Review Committee.

Definitions

a. Anonymized Data. Integrated data that do not include Personal Identifiers. The specific set of Personal Identifiers that must be removed from Anonymized Data are established by each LINC Data Provider in a separate legal agreement with OIT. LINC will use the most restrictive definition of Anonymized Data among all LINC Data Providers contributing data to the LINC Project in this DUL.
b. Authorized Personnel: The members of the LINC Data Recipient team who have been listed in this DUL as having approved access to the LINC Project data and agree to abide by the terms of this DUL.
c. LINC Data Provider: An organization that has direct responsibility for a source of data contributed to the approved LINC Project. This may be an Office or Division of a larger organization, in other cases it may be the organization itself.
d. LINC Data Recipient: The individual or organization that made the approved LINC request for data analysis, research, or evaluation purposes. The LINC Data Recipient will be an employee from a LINC Party or an external researcher.
e. LINC Director: The individual who is responsible for facilitating LINC committees, developing and managing partnerships with Party organizations, overseeing LINC staff, consulting with data requestors, monitoring LINC Projects, and managing the inventory of documents associated with LINC operations and LINC Projects.
f. LINC Project: A project approved by the LINC Review Committee that is analytic, research or evaluative in nature. A LINC Project requires data from two or more Data Providers and must be achievable by LINC Data Recipients with Anonymized Data.
g. LINC Project Data: Anonymized Data for use by the LINC Data Recipient. These data are only to be used for the approved purposes outlined in the approved LINC Request Form.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

h. LINC Request Form: The document that is reviewed by the LINC Review Committee for approval, revision or rejection decisions. The approved LINC Request Form is attached to this DUL as Exhibit 1.
i. LINC Review Committee: The committee composed of representatives from each LINC Data Provider with program or policy expertise and data expertise. At least one of these representatives must have decision-making authority over the use of their data.
j. Personal Identifiers: Any information about an individual that can directly or indirectly distinguish or trace an individual's identity, associate or link an individual to private information, distinguish one person from another, or be used to re-identify individuals.

Financial Understanding

The LINC Data Recipient agrees to pay a fee of _____ to be invoiced upon secure transfer of the LINC Project Data. Payment is expected to be executed within 30 days of receipt of invoice.

2. Permitted LINC Project: Approved Use and Data Elements

This DUL pertains to the LINC Project _____ This LINC Project was approved by the LINC Review Committee on _____ and the approved LINC Request Form is attached and incorporated into this DUL as Exhibit 1. The approved LINC Request Form details the permitted use of the LINC Project Data as well as the approved data elements to be included in the LINC Project Data.

The LINC Data Recipient shall not use the LINC Project Data for any purpose independent of, separate from or not directly connected to the purpose(s) specifically approved by the LINC Review Committee. The LINC Data Recipient shall only receive Anonymized Data and will not be permitted to receive any Personal Identifiers.

3. Data Ownership and Accuracy

LINC Data Recipient acknowledges that LINC Data Recipient has no ownership rights with respect to the LINC Project Data, and that the LINC Data Recipient may only receive and use the LINC Project Data for the purposes approved by the LINC Review Committee.

The LINC Project Data is current as of the date and time compiled and can change. The LINC Data Providers do not ensure 100% accuracy of all records and fields. Some data fields may contain incorrect or incomplete data. OIT and LINC Data Providers cannot commit resources to explain or validate complex matching and cross-referencing programs. LINC Data Recipient accepts the quality of the data they receive. Questions related to LINC Project Data completeness (i.e., approved data elements in the attached Exhibit 1 were received) or matching accuracy shall be sent to the LINC Director within sixty (60) days of receipt. Data that has been manipulated or reprocessed by the LINC Data Recipient is the responsibility of the LINC Data Recipient. OIT cannot commit resources to assist LINC Data Recipient with converting data to another format or answering questions about data that has been converted to another

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

format. Additional issues with the LINC Project Data shall be noted in the Regular Project Report(s) (described in Section 9 below).

4. Data Transfer

LINC Project Data will be transferred to the LINC Data Recipient through a Secure File Transfer Protocol (SFTP) provided or approved by OIT. The LINC Data Recipient will be provided secure access to the SFTP and will be allowed to download the LINC Project Data file(s) for a limited period of time after which access to the SFTP will be removed.

5. Safeguarding Data

Security Controls. The LINC Data Recipient shall implement and maintain the data security controls specified in the LINC Request Form (attached as Exhibit 1) that has been approved by the LINC Review Committee.

Re-Disclosure of Data. LINC Data Recipient shall not use the LINC Project Data for any purpose beyond that specified in Exhibit 1, attached hereto. Furthermore, LINC Data Recipient shall not use the LINC Project Data in an attempt to track individuals, link to an individual's data from other data sources, determine real or likely identities, gain information about an individual or contact any individual (or next-of-kin) who is the subject of the LINC Project. Re-disclosure of data shall result in the immediate suspension of the LINC Project and possible termination of the LINC Project by the LINC Review Committee. Furthermore, individuals engaging in re-disclosure of data will not be approved Authorized Personnel on future LINC Projects.

Cell Suppression Policy. The LINC Data Recipient agrees that any use of LINC Project Data in the creation of any dissemination materials (manuscript, table, chart, study, report, presentation, etc.) concerning the specified purpose must adhere to the cell size suppression policy as follows. This policy stipulates that no cell (e.g., grouping of individuals, patients, clients) with less than _____ observations may be displayed. This is the most stringent cell size allowable among the LINC Data Providers for the LINC Project specified in the approved LINC data request in Exhibit 1. Also, no use of percentages or other mathematical formulas may be used if they result in a cell displaying less than ____ observations. Individual level records may not be published in any form, electronic or printed. Reports and analytics must use complementary cell suppression techniques to ensure that cells with fewer than ____ observations cannot be identified by manipulating Data in adjacent rows, columns or other manipulations of any combination of dissemination materials generated through this LINC Project. Examples of such data elements include, but are not limited to, geography, age groupings, sex, or birth or death dates.

6. LINC Project Authorized Personnel

Any person or entity that processes or receives the LINC Project Data and its agents must be obligated, by contract, to adhere to the terms of this DUL and agree to follow the data security controls approved in the attached Exhibit 1, prior to being granted access to LINC Project Data.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

The following named individuals, and only these individuals, will have access to the LINC Project Data. The LINC Data Recipient will submit a LINC Project Change Request to the LINC Director when an individual leaves the project. The LINC Data Recipient will obtain written approval from the LINC Director for additions to this list prior to granting access to LINC Project Data.

Name	Role	Organization

7. Accountability: Unauthorized Access, Use, or Disclosure

LINC Data Recipient shall take all steps necessary to identify any use or disclosure of LINC Project Data not authorized by this DUL. The LINC Data Recipient will report any unauthorized access, use or disclosure of the Data to OIT via the LINC Director within two business days from learning or should have learned of the unauthorized access, use, or disclosure. In the event that OIT determines or has a reasonable belief that the LINC Data Recipient has made or may have made use or disclosure of the LINC Project Data that is not authorized by this DUL, OIT may, at its sole discretion, require the LINC Data Recipient to perform one or more of the following, or such other actions as OIT, in its sole discretion, deems appropriate:

a. promptly investigate and report to OIT the LINC Data Recipient's determinations regarding any alleged or actual unauthorized access, use, or disclosure;
b. promptly resolve any issues or problems identified by the investigation;
c. submit a formal response to an allegation of unauthorized access, use, or disclosure;
d. submit a corrective action plan with steps designed to prevent any future unauthorized access, use, or disclosures; and
e. return all LINC Project Data or destroy LINC Project Data it has received under this DUL.

The LINC Data Recipient understands that as a result of OIT's determination or reasonable belief that unauthorized access, use, or disclosures have taken place, OIT may refuse to release further LINC Project Data to the LINC Data Recipient for a period of time to be determined by OIT, in its sole discretion.

8. LINC Project Reporting Requirements

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

Regular Project Reports. LINC Data Recipients must submit Regular Project Reports to the LINC Review Committee, annually or at the midterm point of the project cycle, whichever comes first. The report shall be a standard form automatically distributed by the LINC Director or support staff and shall require:

a. IRB approval documentation
b. Summary of progress to date
    - How project is informing policy or practice
    - Description of anticipated and unanticipated findings
    - Description of challenges encountered and how they are being resolved
c. Dissemination materials and key findings to date
d. Project funding source (if applicable)

Change Requests. LINC Data Recipients will initiate, when necessary, a LINC Project change request. Minor requests (e.g., change in key personnel, a first-time extension of up to six months) will be reviewed by the LINC Director. Major requests (e.g., additional research questions; change in organization using data) will be reviewed by the LINC Review Committee.

Key Findings and Interpretations Release Request. LINC Data Recipients are required to share LINC Project findings to the LINC Review Committee prior to any public release. LINC Review Committee members have the right to request that their organization be anonymized in any publications. LINC Data Recipients shall submit key findings and interpretations in a standard format provided by the LINC Director or support staff. LINC Review Committee members shall confirm in writing, via a standard form provided by the LINC Director, that key findings have been reviewed and are ready for release. The LINC Review Committee members can request review of specific dissemination materials (e.g., presentations, publications).

LINC Acknowledgement. All publicly-released materials resulting from the LINC Project referenced in this DUL shall include the following acknowledgement: “This work would not be possible without anonymized data provided by the Linked Information Network of Colorado (LINC) in the Colorado Governor’s Office of Information Technology. The findings do not necessarily reflect the opinions of the Colorado Governor’s Office of Information Technology or the organizations contributing data.”

Final Publication(s). The LINC Data Recipient shall provide the LINC Director with an electronic copy of all published work resulting from the LINC Project associated with this DUL within 30 days of publication.

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

9. Data Retention and Destruction

The LINC Data Recipient agrees to destroy all LINC Project Data by the approved LINC Project end date, in accordance with the "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," as established by the U.S. Department of Health and Human Services (HHS). The LINC Data Recipient may request an extension of the Data Retention Period by submitting a written request that includes justification to the LINC Review Committee via the LINC Director. This extension request must be submitted 30 days prior to the LINC Project end date.

When retention of the LINC Project Data is no longer justified, the LINC Data Recipient agrees to destroy the Data and send a completed "Certification of Project Completion & Destruction of Data" form (Attachment 1 to this Agreement) to OIT via the LINC Director by the approved LINC Project end date. The LINC Data Recipient agrees not to retain any LINC Project Data, or any parts thereof, or any derivative files that can be used in concert with other information after the aforementioned file(s) and LINC Project Data are destroyed unless the LINC Review Committee grants written authorization. The LINC Data Recipient acknowledges that such date for retention of LINC Project Data is not contingent upon action by OIT.

10. Term and Termination

By signing this DUL, the LINC Data Recipient agrees to abide by all provisions set out in this DUL. This DUL will become effective upon the last date of execution by OIT and the LINC Data Recipient to this DUL. Unless terminated sooner pursuant to Sections 6 and 8 above, this DUL will remain effective in its entirety until the completed "Certification of Project Completion & Destruction or Retention of Data" has been received by the OIT.

[*Remainder of this page left intentionally blank*]

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

11. Signature

The effective date of the DUL shall be _____, 20 ___. The DUL will remain in effect until _____, 20 ___.

IN WITNESS WHEREOF, the Party hereto have caused this Agreement to be executed by their duly authorized representative.

[NAME]

_____ Dated: _____

[TITLE]

[ORGANIZATION]

DocuSign Envelope ID: A8E405A2-BFD6-4635-9CAB-B838A2DB5AD5

LINC DUL Attachment 1:

Linked Information Network of Colorado (LINC)
Certification of Project Completion and Data Destruction

The LINC Data Use License (DUL) signed by _____ ("Data Recipient") on _____ date for LINC Project #_____ allowed for the receipt of anonymized LINC Project data during the project period. The Principal Investigator (PI) and/or Co-Principal Investigator (Co-PI) identified in the LINC DUL is required to destroy all data provided for the approved LINC Project by the end date of the project specified in the LINC DUL. In the DUL, the LINC Data Recipient agreed not to retain any LINC Project Data, or any parts thereof, or any derivative files that can be used in concert with other information after the aforementioned file(s) and LINC Project Data.

By signing below, the PI or Co-PI assures that all data elements loaned to the authorized personnel listed in the DUL for LINC Project #19-01 have been destroyed in accordance with the "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," as established by the U.S. Department of Health and Human Services (HHS). The details of data destruction are as follows:

1. Data destruction date:

2. Data destruction personnel:

3. Data destruction method:

Signature: _____ Date: _____

LINC Project #_____

PI/Co-PI Name: _____

Organization: _____

Phone Number: _____. Email address: _____

Address: _____

Please send the signed and completed form to:
Whitney LeBoeuf, LINC Director (whitney@coloradolab.org)