Research Data Sharing Agreement between the Colorado Department of Education (CDE) and [Insert Name of Entity]

This Research Data Sharing Agreement (Agreement) is entered into by and between the Colorado Department of Education (CDE), 201 E. Colfax Avenue Denver, CO 80203 and [Insert Name of Entity] (Researcher), whose address is [insert address here] individually a Party and together the Parties.

I. Definitions

A. "Aggregate Data" means data collected and reported at the group, cohort, or institutional level that is aggregated using protocols that are effective for preserving the anonymity of each individual included in the data.

B. "Data" includes Student Personally Identifiable Information and Educator Data.

C. "Data Breach" means unauthorized or unintentional use, exposure, disclosure, or loss of Data.

D. "Data Governance" means the oversight of data quality, data management, data policies, business process management, and risk management surrounding the handling of Data, and includes a set of processes that ensures that important Data assets are formally managed throughout the Party's department, organization, or enterprise.

E. "Data Governance Manager" means the individual responsible for the implementation and oversight of the Party's data management goals, standards, practices, processes, and policies.

F. "Data Owner" is the individual with responsibility and authority for an entrusted data resource. The data owner takes ownership of the operational, technical, and informational management of the PII.

G. "Destroy" means to remove Data from Researcher's systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in NIST Special Publication 800-88 Guidelines for Media Sanitization so that Data is permanently irretrievable in the Researcher's normal course of business.

H. "Educator Data" includes, but is not limited to, the educator's name; any unique identifier, including social security number; and other information that, alone or in combination, is linked or linkable to a specific educator.

I. "Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g" means the federal law that protects the privacy of students' personally identifiable information.

J. "Incident" means an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources of the State.

Incidents include, but are not limited to (i) successful attempts to gain unauthorized access to a State system or Data regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a State system for the processing or storage of data; (iv) changes to State system hardware, firmware, or software characteristics without the State's knowledge, instruction, or consent; or (v) a breach of this Agreement that results in the misuse or unauthorized disclosure of Data.

K. "Student Personally Identifiable Information (PII)" means information that is collected, maintained, generated, or inferred and that, alone or in combination, personally identifies an individual student or the student's parent or family. PII also includes other information that, alone or in combination, is linked or linkable to a specific student that would 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; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

L. "Subcontractor" means any third party engaged by Researcher to aid in performance of a study or evaluation described in an appendix to this Agreement.

M. "System Steward" means the entity responsible for combining two data sets from different sources and managing the resultant data set. If a CDE data system is being used, then CDE is the System Steward. If another entity is doing the calculations or derivations, then that entity becomes the System Steward.

N. "Targeted Advertising" means selecting and sending advertisements to a student based on information obtained or inferred over time from the student's online behavior, use of applications, or PII. Targeted Advertising does not include advertising to a student at an online location based on the student's current visit to that location or in response to the student's request for information or feedback and is without the collection and retention of a student's online activities over time. Targeted Advertising also does not include adaptive learning, personalized learning, or customized education.

II. Purpose and Scope of Agreement

A. CDE is the state education agency responsible for the implementation of education laws adopted by the State of Colorado. In fulfillment of law found in the Colorado Revised Statutes, CDE is charged with collecting and securely maintaining data on students enrolled in the state's Local Education Providers (LEPs).

B. This Agreement applies to all data sharing between Researcher and CDE. Specific data to be shared are outlined in attached appendices, along with the purpose of data sharing, data ownership and conditions and/or regulations governing the usage of the shared data, requirements for

shared data retention/destruction, and Party processes for implementing these actions.

C. This Agreement will be reviewed, updated, and approved on an annual basis.

D. This Agreement sets forth the terms under which CDE is authorized to release Data, including Student PII, to Researcher for approved research pursuant to CDE's Personally Identifiable Information Protection policy and in compliance with the Family Educational Rights and Privacy Act (FERPA), Colorado's Student Data Transparency and Security Act, and any other pertinent federal or state statutes and regulations. FERPA Exceptions will be specified in the individual Use Cases/Appendices.

III. General Provisions

A. CDE reserves all right, title, and interest, including all intellectual property and proprietary rights, in and to Data and all related content.

B. Researcher shall comply with FERPA, Colorado's Student Data Transparency and Security Act, and any other pertinent federal or state statutes and regulations.

C. Researcher shall immediately forward to CDE's principal representative any request or demand from a third party for Data in the possession of Researcher.

D. Upon request of CDE or of the Colorado State Board of Education, Researcher shall submit its data processing facilities for an audit of the measures referred to in this Agreement by CDE or by a CDE-approved delegate.

E. Researcher shall send CDE a written notice that includes a clear explanation of the proposed changes prior to making a material change to Researcher's privacy policies.

IV. Use of Data

A. Researcher shall not use or share Data beyond the purposes set forth in the Appendices. Any request to use or share Data outside of this Agreement must be submitted in writing to CDE and CDE and Researcher will have to amend this Agreement or add additional Appendices that fully describe the new uses or sharing of Data.

B. In the event the Agreement requires Researcher to store, process or transfer Data, Researcher shall store, process, and transfer Data only in or to facilities located within the United States.

C. During the term of this Agreement, if CDE requests the destruction of a student's PII collected, generated or inferred as a result of this Agreement, Researcher shall Destroy the information within five calendar days after the date of the request unless:

1. Researcher obtains the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian to retain the student's PII; or

2. The student has transferred to another state and the receiving state has requested that Researcher retain the student's PII.

D. If Researcher seeks to share or publicly release Data, Researcher must de-identify or aggregate the PII prior to releasing the data publicly. The following requirements apply for Data to be considered Aggregate Data:
   1. Data to be aggregated or de-identified shall include not only direct identifiers, such as names, student IDs or social security numbers, but also any other sensitive and non-sensitive information that, alone or combined with other information that is linked or linkable to a specific individual, would allow identification.
   2. Simple removal of direct identifiers from the Data to be released shall not constitute adequate de-identification.
   3. Researcher shall de-identify Data to remove cumulative re-identification risks.
   4. Researcher shall remove all Data that in conjunction with previous data releases and other reasonably available information, including publicly available directory information and de-identified data releases from education records and other sources would allow for identification of a particular student.
   5. Researcher shall have specific steps and methods used to de-identify or aggregate Data to protect the confidentiality of individuals. Researcher shall, at the request of CDE, provide CDE with a document that lists the steps and methods Researcher shall use to de-identify Data.

E. Prior to public dissemination/release, Researcher shall provide reports or documentation generated as a result of using Data received from CDE to permit the CDE to verify that the intended purpose has been adhered to and that the publication has been appropriately aggregated or de-identified. CDE will ensure that access to the report is permitted on a need-to-know basis only for this verification purpose and will protect the report from public dissemination or release.

F. CDE reserves the right to receive a final copy of the research report and post that report on CDE's public facing website.

G. If receiving Educator Data, Researcher shall comply with the provisions of C.R.S. § 24-74-101 et. seq.)

V. Disallowed Activities

A. Researcher shall not disclose Data to any third party except for the authorized Subcontractors identified in an appendix to this Agreement.

B. Researcher may not use Data in a manner that is inconsistent with Researcher's privacy policy.

C. Researcher shall not sell Data, except that this prohibition does not apply to the purchase, merger, or other type of acquisition of Researcher, or any assets of Researcher, by another entity, so long as

the successor entity continues to be subject to the provisions of this Agreement.

D. Researcher shall not use or share Data with any party for the purposes of Targeted Advertising to students.

E. Researcher shall not use Data to create a personal profile of a student other than for supporting the purposes authorized by CDE or with the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian.

F. Researcher shall not publish reports with a cell size of less than 16 or that includes Data that has not been aggregated or de-identified as specified in this Agreement. Any Data that is not properly de-identified or aggregated and is publicly released by Researcher will be considered an Incident.

G. Researcher shall not maintain or forward PII to or from any other facility or location outside of the Researcher's organization.

H. There shall be no disclosure of Data to government agencies outside of the state.

VI. Data Security

A. Researcher shall maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of Data. At a minimum, the information security program shall include the requirements listed in this Section VI – Data Security.

B. Researcher shall provide physical and logical protection for all related hardware, software, applications, and data that meet or exceed industry standards and requirements as set forth in this Agreement. Researcher shall take full responsibility for the security of all Data in its possession, and shall hold CDE harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof. Researcher shall provide for the security of Data, in a form acceptable to CDE, including, without limitation, non-disclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, network firewalls, intrusion detection (host and network), data security logging and monitoring systems, and audits.

C. Researcher shall provide CDE or its designated representatives with access, subject to Researcher's reasonable access security requirements, for the purpose of inspecting and monitoring access and use of Data and evaluating physical and logical security control effectiveness.

D. Researcher shall perform, in a form reasonably acceptable to CDE, current background checks on all of its respective employees and agents identified as requiring access to Data in the Appendices. The background checks must include, but are not limited to the following areas: County, State, National and Federal Criminal Records and a Sex Offender Registry Search. A background check performed within thirty

(30) calendar days prior to the date such employee or agent begins performance or obtains access to Data shall be deemed to be current.

E. Researcher shall have strong access controls, including role-based access to ensure that only authorized individuals have access to Data.

F. Workstations and other data processing devices must automatically lock when not in use and must be manually locked when left unattended.

G. Researcher shall protect all Data with a complex password. Researcher shall ensure passwords are confidential and prohibit the sharing of passwords. Passwords must not be written down or stored in an unsecure location. Researcher shall periodically change passwords and shall ensure passwords are not reused. Researcher shall have password locks for laptops and mobile devices.

H. Researcher shall disable and/or immediately delete unused and terminated user accounts. Researcher shall periodically assess account inactivity for potential stale accounts.

I. Researcher shall not share Data on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes.

J. Researcher shall implement annual intrusion penetration/vulnerability testing.

K. Researcher shall encrypt Data at rest on central computing systems. Researcher shall also encrypt any backup, backup media, removable media, tape, or other copies. In addition, Researcher shall fully encrypt disks and storage for all laptops and mobile devices.

L. Researcher shall provide annual, mandatory security awareness and Data handling training for all of its employees handling Data pursuant to this Agreement.

M. Researcher shall install and maintain on computers accessing or processing Data appropriate endpoint security anti-virus and anti-malware software. Researcher shall ensure all Researcher's data processing systems, servers, laptops, PCs, and mobile devices are regularly scanned and have all security patches applied in a timely manner.

N. Researcher shall use a secure method such as Secure File Transfer Protocol (SFTP) or comparable method to transmit Data. Researcher shall never send Data via email or transport Data on removable media.

O. Researcher shall have physical security in buildings housing Data, along with controlled physical access to buildings and/or data centers.

P. Researcher's devices used to copy or scan hard copies of Data must have encrypted storage. Researcher shall scrub storage devices when equipment is retired. Hard copies containing Data are discouraged and must be physically secured, not left unattended, and physically Destroyed.

Q. Researcher shall protect Data stored in cloud-based systems in the same manner as local Data. Use of free cloud-based services is prohibited. Data shall use secondary encryption to protect Data in cloud storage.

Cloud environments, when employed by Researcher, must be fully documented by Researcher and open to CDE inspection and verification. Access to Researcher's cloud-based computing environments is only permitted via restricted access, by VPN or least privileged access lists, and never accessible directly via the Internet.

VII. Transparency Requirements

A. Researcher shall facilitate access to and correction of any factually inaccurate student PII in response to a request from a LEP or from CDE.

B. Researcher acknowledges that CDE will post this Agreement to CDE's website.

VIII. Data Governance Plans

A. Researcher agrees to have in place a Data Governance plan with support and participation from across the organization that details the organization's policies and procedures to protect privacy and data security, including ongoing management of data collection, processing, storage, maintenance, use, and destruction. CDE has the right to conduct audits or other monitoring of Researcher's Data Governance policies, procedures, and systems.

B. If, through these monitoring activities, vulnerability is found, Researcher must take timely appropriate action to correct or mitigate any weaknesses discovered. If Researcher's current data security policies and procedures are not posted on an externally facing website, they will be provided to CDE prior to the signature of this Agreement and annually thereafter and must include the minimum security policies and procedures set forth below:

1. Privacy and Security Policies and Procedures
2. Identification of a Privacy and Security Board and Officer
3. Management Oversight of Privacy and Security Programs
4. Sanctions for Violations of Policies and Procedures
5. Reporting Potential Problems in Privacy and Security
6. Incident Response and Incident Response Mitigation
7. Privacy and Security Training
8. Access Control, Minimum Necessary Access and Verification for Access to Data
9. Password Management
10. Transmitting Sensitive Information Securely including Faxing and Email
11. Log-in Monitoring
12. Workstation Security Configuration
13. Device and Media Control
14. Securing Materials with Data
15. Encryption
16. Authorizations for Personal Health Information, if applicable
17. Permitted Uses and Disclosures of PHI, if applicable

18. HIPAA Status, if applicable
19. Business Associate Status, if applicable
20. Designating Sensitive Information
21. Risk Assessments and Management
22. Change Control Procedures
23. Audit and Evaluation Procedures

IX. Data Retention and Destruction

A. CDE may terminate this Agreement at any time, for its own convenience, for any reason, with written notice to the Researcher. The Researcher may terminate this Agreement for any reason, with thirty (30) days written notice to CDE.

B. Upon request by CDE made before or within thirty (30) calendar days after termination of the Agreement, Researcher shall make available to CDE a complete and secure (i.e. encrypted and appropriately authenticated) download file of all Data.

C. CDE retains the right to use the established operational services to access and retrieve Data stored on Researcher's infrastructure at its sole discretion.

D. Following the termination of this Agreement, Researcher shall, within thirty (30) calendar days, Destroy all Data collected, generated, or inferred as a result of this Agreement. Researcher shall certify to CDE in writing that the Data has been Destroyed.

X. Individual Duties

A. All involved Data Owners will participate in the determination to provide Data based on CDE polices and applicable laws and regulations. Data Owners will also participate in any validation and risk assessments as defined in this Agreement.

B. The Data Owner takes ownership of the operational, technical, and informational management of the Data.

C. Each Party's Data Governance Manager is authorized, after following approved internal Data Governance policies, to approve the use of Data.

D. The System Steward shall manage the source system and ensure the integrity and safety of the Data at all times.

E. The System Steward shall follow all security requirements outlined in this Agreement, to prevent the use or disclosure of Data not authorized by either this Agreement or the attached appendices.

F. The System Steward agrees to abide by all applicable state and federal laws and regulations, including FERPA, Colorado's Student Data Transparency and Security Act, and others as specified in attached Appendices.

XI. Data Linkage

A. If Researcher will link CDE's Data with Data from another source, the result could be a new data set with potentially unique regulations and conditions governing its use. Prior to linking the Data, Researcher will provide detailed information to CDE outlining the Data being linked and the other sources for Data.

B. The System Steward will classify the linked data based on security or privacy risks. This could include evaluating the method of release, on the likelihood of identifying individuals from the linked Data, if linking the Data will violate any laws or regulations, or if the new data set meets the original request.

C. Based on the results of the risk assessment, CDE may refuse to provide Researcher with some or all of the requested Data in its sole discretion in order to mitigate any risks identified.

D. Should CDE consent to the Data being linked, the System Steward shall apply additional constraints as necessary to the usage of the new data set.

E. Detailed information on the Data being linked, the other sources of Data, and any additional constraints shall be documented in the Appendix.

XII. Unauthorized Uses, Disclosures or Breaches

A. If Researcher becomes aware of an Incident, misuse of Data, or unauthorized disclosure involving any Data, it shall notify CDE within one (1) calendar day and cooperate with CDE regarding recovery and remediation of the Incident, and the necessity to involve law enforcement, if any.

B. Researcher shall determine the cause of an Incident and produce a remediation plan to reduce the risk of incurring a similar type of breach in the future. Researcher shall present its analysis and remediation plan to CDE within ten (10) calendar days of notifying CDE of an Incident. CDE reserves the right to adjust this plan, in its sole discretion. If Researcher cannot produce its analysis and plan within the allotted time, CDE, in its sole discretion, may perform such analysis and produce a remediation plan, and Researcher shall reimburse CDE for the reasonable costs thereof.

C. Unless Researcher can establish that Researcher is not the cause or source of the Incident, Researcher shall be responsible for the cost of notifying each person whose Data may have been compromised by the Incident.

D. Disclosure of Data by Researcher for any reason may be cause for legal action by third parties against Researcher, CDE, or their respective agents. Researcher shall indemnify, save, and hold harmless CDE, its employees, and agents against all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred because of any act or omission by Researcher, or its employees, agents,

Subcontractors, or assignees pursuant to this Agreement. Notwithstanding any other provision of this Agreement, Researcher shall be liable to CDE for all direct, consequential, and incidental damages arising from an Incident caused by Researcher.

E. In the event of an Incident, Researcher shall provide CDE or its designated representatives with access seven (7) days a week, twenty-four (24) hours a day, for the purpose of evaluating, mitigating, or resolving the Incident.

XIII. Data Accuracy

A. The Data provided are the best and most complete documentation available. CDE does not ensure 100% accuracy of all records and fields. Some data fields, including those that are not used, may contain incorrect or incomplete Data. CDE and Researcher will report any systematic problems with the Data to the Data Owner. Data that has been manipulated or re-processed by either CDE or Researcher is the responsibility of that Party.

XIV. Non-Financial Understanding

A. This Agreement is a non-financial understanding between CDE and Researcher. No financial obligation by or on behalf of either of the parties is implied by a party's signature at the end of this Agreement.

B. The terms of any financial liability that arises from data processing activities carried out in support of the responsibilities covered herein must be negotiated separately and to the mutual satisfaction of the Parties.

C. The legal authority for data sharing for specified purposes conveyed by this Agreement cannot be used to support a subsequent claim of implied agreement to financial obligation.

XV. Insurance

A. Researcher shall obtain and maintain insurance as specified in this section at all times during the term of this Agreement. All insurance policies required by this Agreement shall be issued by insurance companies as approved by the State.

1. Protected Information Insurance. Liability insurance covering all loss of State Confidential Information, such as PII, PHI, PCI, Tax Information, and CJI, and claims based on alleged violations of privacy rights through improper use or disclosure of protected information with minimum limits as follows:
    i. $1,000,000 each occurrence; and
    ii. $2,000,000 general aggregate.
2. Cyber Privacy Insurance. Researcher agrees to maintain Cyber Privacy Insurance for claims and losses with respect to network, internet (cloud) or other data disclosure risks (such as data breaches, releases of confidential information, unauthorized

access/use of information, and identity theft) with minimum limits of not less than:

i. $1,000,000 per each occurrence; and
ii. $2,000,000 aggregate.

XVI. Survival

A. The respective rights and obligations of parties shall survive the termination of this Agreement with respect to Data previously shared.

XVII. Effective Date and Term

A. This Agreement shall take effect upon its signing by all Parties.
B. This Agreement may be amended at any time by mutual agreement of all Parties.
C. All parties will conduct an independent review of this Agreement on an annual basis.
D. This Agreement shall remain in effect until [insert date here] unless terminated by written notification from one party to another.
E. CDE, at its sole discretion upon written notice to Researcher, may unilaterally extend the term of this Data Sharing Agreement for a period not to exceed two months if the Parties are negotiating a term extension or subsequent Data Sharing Agreement at or near the end of any initial term or renewal term. The provisions of this Data Sharing Agreement in effect when such notice is given shall remain in effect during the two-month extension. The two-month extension shall immediately terminate when and if a subsequent Data Sharing Agreement is approved and signed by the Parties.

XVIII. Signatures

To further the collection and analysis of Colorado educational Data, CDE and Researcher agree to the cooperative sharing of Data between the Parties pursuant to the conditions set forth herein.

Signature:
Date:
Susana Córdova
Commissioner of Education
Colorado Department of Education

Signature:
Date:
[Insert name here]
Insert title here]
[Insert organization here]

APPENDIX A – [Insert Project Title Here]

I. Purpose

A. [Insert a detailed summary of the purpose for requesting the data, information about the purpose of the researcher and any other background applicable to the research being conducted.]

II. Disclosure Allowances by Statute

A. CDE is a State Educational Authority under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g; and 34 C.F.R. Part 99, that is authorized to access, copy, use, and disseminate student educational records and receive information from local educational agencies consistent with FERPA and other laws. The general rule under FERPA is that PII from education records cannot be disclosed without consent, subject to certain exceptions.

B. FERPA's audit and evaluation exception allows for the disclosure of PII from education records to authorized representatives of the Comptroller General of the U.S., the Attorney General, the Secretary of Education, and state or local LEAs in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. 20 U.S.C. 1232g(b)(1)(C), (B)(3), and (b)(5) and §§99.31(a)(3) and 99.35.

CDE and Researcher agree that Researcher is an individual or organization to whom CDE can disclose student PII from educational records without consent under FERPA's audit and evaluation exception.

C. CDE designates Researcher as an Authorized Representative for purposes of disclosing student information, including PII, for use as described in this Appendix, under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g; and 34 C.F.R. Part 99.

D. CDE will disclose to Researcher the Data listed in Section IX. Required Data of this Appendix.

E. The purpose for disclosure of the student PII to Researcher is to carry out an audit or evaluation of Federal or State supported education programs. Researcher will be conducting an evaluation [insert brief description here of the federal or state supported education programs], as described in this Appendix. Data use will be governed by the terms of this Agreement and Appendix. Researcher may only use the data for purposes authorized by this Agreement and Appendix.

F. Researcher shall not disclose Data to any third parties.

III. Roles

A. The System Steward for this use case is Researcher.

B. The Data Governance Manager for CDE is Marcia Bohannon and the Data Governance Manager for Researcher is [insert name here].

C. Data may only be accessed, viewed, or used by the Researcher's staff identified in this Appendix. Researcher may identify additional staff who

require access to Data and provide that request to CDE in writing for review and consideration. Researcher's staff with permission to view, access, or use Data include: [insert names here]

IV. Request

A. [Insert a summary of what data is being collected, the reason why this research requires personally identifiable information, and the purpose for collection.]

V. Output

A. [Insert a summary of the output. This section states what reports or information will be produced because of this research and where that information will go.]

VI. Data Linkage

A. [Insert detailed information on the Data being linked, the other sources of Data, and any additional constraints to protect the linked Data.]

VII. Participating Parties

A. The Colorado Department of Education (CDE) will be sharing data with [Insert Organization Name].

VIII. Duration of Study

A. The study referenced in this Appendix will end on [insert date here]. The shared Data for this study must be Destroyed by [insert date here] and Researcher must notify CDE when destruction is complete.

IX. Required Data

A. [Insert List of Data Here]

X. Research Questions, Variables of Interest, and Analytic Approach

A. Study Research Questions
1. [Insert Research Questions]

B. Outcomes Variables
1. [Insert Specific Variables]

C. Analysis
1. [Describe analysis here]

XI. Regulations that Apply

A. FERPA (34 CFR Part 99)

B. The Student Data Transparency and Security Act (C.R.S. § 22-16-101 et. seq.)

XII. Signatures

To further the collection and analysis of Colorado educational Data, CDE and Researcher agree to the cooperative sharing of Data between the Parties pursuant to the conditions set forth herein.

Signature:
Date
Susana Córdova
Commissioner of Education
Colorado Department of Education

Signature:
Date:
[Insert name here]
Insert title here]
[Insert organization here]