Table of Contents

Revisions

Version	Date	Change	Name
Draft 0.1	8.13.14	First draft for CDPS review	Wass
Draft 0.2	9.11.14	Draft for CDE, DSA Committee Review & Feedback	Jorgensen
Draft 0.3	10.10.14	Feedback provided from review committee for resend to CDPS	Markel, Jorgensen
Draft 0.4	10.28.14	Received CDPS DSA with agreement to language; resent to Carey for final approval and then it will be directed back to Tara Wass for signatures.	Wass, Jorgensen
	10.29.14	Approved via e-mail; sent for signatures to Tara on 10-31-14	Markel

Data Sharing Agreement Between the Colorado Department of Education (CDE) and the Colorado Department of Public Safety (CDPS)

This Data Sharing Agreement (Agreement) is entered into by and between the Colorado Department of Education (CDE), 201 E. Colfax Avenue Denver, CO 80203 and the Colorado Department of Public Safety (CDPS), 700 Kipling St. #1000, Denver, CO 80215, each individually a party and together the parties.

I. Scope of Agreement

CDE is a 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 unit record data on students enrolled in the state's Local Education Agencies (LEAs). The CDPS is responsible for providing help to sheriffs, police and fire departments, and emergency managers whenever local officials request assistance. CDPS also conducts research and policy analyses to assist the Department in its support and enforcement activities. This Agreement applies to all data sharing between CDPS 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. Also in the appendix will be further requirements for shared data retention/destruction, and agency processes for implementing these actions.

II. Purpose

CDE and CDPS enter into an interagency agreement on or about September 1, 2014 to share and exchange Data for the purposes of: (1) conducting educational studies to develop, validate, or administer predictive tests, administer student aid programs, or improve instruction and (2) to audit or evaluate federal or state supported education programs or to enforce or comply with federal legal requirements that relate to those education programs. Details of the data to be shared are outlined in the appendices. This Agreement is designed to be an umbrella agreement for all data sharing activities between CDE and CDPS. For specific use cases, i.e., detailed data requests for specific research purposes, the details shall be spelled out via an appendix attached to this agreement. The appendices will include:

- The specific data requested for a particular use case;
- The roles of the Data Provider (defined below) and Data Consumer (defined below) for the particular use case;
- The individual(s) that will be directly responsible for managing the data in question;
- The purpose for which the data is being requested;

- How the data will be used and why disclosure of Personally Identifiable Student Data (defined below) is necessary to carry out that purpose;
- Whether or not the use case requires data linking; and
- Information about relevant laws or guidelines to be followed when sharing or working with the data, including the technical, physical and administrative safeguards that will be used to protect Personally Identifiable Data at rest and in transit.

This Agreement shall be used exclusively for the purposes of sharing Data as permitted by the Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and any other pertinent federal or state statutes and regulations. Said state statutes and regulations include the Data Governance rules and policies for security and privacy found at: http://www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1249667675596.

III. Definitions

Authorized User means an individual who has been granted the appropriate privileges and rights to access an information technology system and view the data contained within (as defined in the respective department's data sharing policy).

Data means the representation of facts as texts, numbers, graphics, images, sounds, or video. Facts are captured, stored, and expressed as Data.

Data Breach means unauthorized or unintentional exposure, disclosure, or loss of private public information, which may include personally identifiable information.

Data Consumer means an individual who receives, analyzes and reports results of data from the Data Provider. In the case of educational longitudinal data linking research, a researcher submitting a question would be the Data Consumer.

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 State Agency, department organization, or enterprise.

Data Governance Manager means the individual responsible for the implementation and oversight of the State Agency's data management goals, standards, practices, processes, and policies. Each Agency's Data Governance Manager is authorized, after following approved internal Data Governance policies, to approve the sharing and release of that State Agency's data to entities outside of that State Agency.

Data Owner means a person having the responsibility and authority for an entrusted data resource. The Data Owner plays a key role in internal Data Governance within each State Agency or Early Childhood Program. The Data Owner takes ownership of the operational, technical, and informational management of the Data. The Data Owner knows how to use the data, to whom it can be released and the appropriate conditions and regulations that govern the use of the data.

Data Provider means the Party that originally collected the Data. Providing information means that data is made available to the Link system, to match with the other Data Providers' data to achieve a match. The matched data set resulting from agreed upon match criteria is the result of linking and becomes our "Linked Data" per the definition below. Data provided will be defined in each Appendix, according to the associated Use Case.

Data Steward means individuals who manage data elements and/or categories at various points in the data lifecycle.

Decision Making using Data means any instance where analysis of data and subsequent results are used to help make an educational, administrative, or other decision.

Demographics, in this agreement, refers to the *minimum* set of data elements that uniquely define a particular person, e.g., name, address, date of birth.

Educational Research means any research designed to address an educational goal, question, or issue.

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.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 and regulations promulgated thereunder by the U.S. Department of Health and Corrections (the "HIPAA Regulations"), means the federal law that establishes privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

K-12 means school education levels ranging from Kindergarten to high school graduation.

Linked Data means the resultant data set after two or more agencies' data have been linked manually or through the RISE Link data system.

Longitudinal Analysis means an analysis of data or a population over time.

Personal Identifying Information (PII) means all the information identified in 34 CFR Part 99, section 99.3, including a person's first name or first initial and last name in combination with his or her social security number or driver's license number or identification number, including address.

Relevant Information to Strengthen Education (RISE); is the brand name applied to the outcomes that will be realized with the implementation of the SLDS Grant, and other data related initiatives.

Risk Assessment of Linked Data is a review conducted of the results of two or more pieces of data linked together by the RISE system to answer a specific educational question. The focus of the Risk Assessment is to determine the level of risk (related to a data breach) introduced by combining data. The individual data providers will participate in the Risk Assessment to help determine if the new data set may have unique regulations and conditions governing its release and use that were not present prior to combining the data. The System Steward and Data Providers will agree on and carry out any additional security or steps that are required as a result of the Risk Assessment to ensure the integrity of the Linked Data, up to and including the decision not to release the linked data.

Role-Based Access means a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.

State Agency means each principal department within the executive branch, including each board, division, unit, office, or other subdivision within each department, each office or agency within the Governor's Office, each state-supported institution of higher education, and each local district junior college; except that State agency shall not include any department, agency, board, division, unit, office, or other subdivision of a department that does not collect unit records.

Statewide Longitudinal Data System (SLDS) means a federal grant program that has helped to propel the successful design, development, implementation, and expansion of K-12 longitudinal data systems to include early learning, post-secondary and workforce.

System Steward means the agency responsible for linking or connecting data elements to form a new linked data set. This refers to CDE when the RISE Link system is utilized. If data is linked manually, the agency responsible for that effort becomes the System Steward. The System Steward will ensure that the provided data will be handled with care, following all

applicable Colorado information security policies. All involved Data Owners will participate in validation and risk assessments as defined in this agreement.

IV. Access Restrictions

A. The parties agree to use role-based access to ensure that only Authorized Users at CDE and CDPS have access to the specific Data needed to complete their work assignment as required by their job responsibilities within the scope of this agreement.

B. The specific records to be released from the Data Provider shall be subject to the consent of the Data Provider's Data Governance Manager (or designated authority).

V. Re-disclosure of Data

A. Without authorization from the Data Governance Manager (or designated authority) of the Data Provider, the Data Consumer may only further disclose data in an aggregate form that does not allow the identification of individuals.

VI. Data Provider Duties

A. The Data Provider shall serve as the Data Owner.

B. The Data Consumer shall not retain any right, title or interest in any of the Data furnished by the Data Provider.

C. The Data Provider maintains ownership in the case of third party vendors who may house agency Data off-site as a part of the longitudinal data linking process.

D. The Data Provider shall ensure that identifying information is transmitted through secured encrypted connections.

VII. Data Consumer Duties

A. The Data Consumer maintains a stewardship role for the preservation and quality of the Data.

B. The Data Consumer may use and disclose Data as permitted in this agreement and only in a manner that does not violate state or federal privacy statutes and regulations.

C. The Data Consumer shall implement appropriate safeguards to prevent use or disclosure of Data not authorized by this agreement.

D. The Data Consumer agrees to abide by all applicable state and federal privacy statutes and regulations.

E. The Data Consumer shall ensure that the Data are kept in a secured environment at all times and that only Authorized Users have access.

F. The Data Consumer shall promptly report to the Data Provider any use or disclosure of the Data of which the Data Consumer becomes aware that is not provided for or permitted in this agreement.

G. The Data Consumer shall permit the Data Provider to investigate any such report and to examine the Data Consumer's premises, records and practices.

H. The Data Consumer agrees to abide by the Data Breach notification procedures, as described in section XV below.

VIII. System Steward Duties

A. Where RISE Link technology is used, the System Steward maintains a stewardship role for the preservation and quality of the Data.

B. The System Steward shall manage the RISE system, if being used to link data, and ensure the integrity and safety of the Data at all times.

C. The System Steward shall implement appropriate safeguards to prevent use or disclosure of Data not authorized by the use cases specified in the attached appendices.

IX. Release of Linked Data to Data Consumer

The result of linking different agencies' (i.e. CDE and CDPS) data sets is a new data set that potentially has unique regulations and conditions governing its release and use. Each Party shall have the right to review any data prior to publication to verify that proper disclosure avoidance techniques have been used and to approve reports prior to publication to ensure that they reflect the original intent of the data sharing outlined for each use case.

- Prior to release of Linked Data, the System Steward will classify the Linked Data according to risk of data breach. This could include evaluating based on means of release, or on

likelihood of identifying personally identifiable information from the Linked Data (or violating other regulations that apply to the Linked Data).

- Based on the above classification, if PII will be released, a full Risk Assessment shall be conducted prior to release. At a minimum, the following questions shall be asked:

    a. Does the Linked Data meet the original request and can it be used in the manner the Data Consumer planned?
    b. What conditions and/or regulations apply to the Linked Data?
    c. Does usage of the Linked Data pose a high risk of breaching those regulations?
    d. Can and will reasonable and appropriate steps be taken to reduce the risk of breach during the actual transfer of data to the Data Consumer?
    e. How will the data be protected at rest and in transit?

- Results of the Risk Assessment shall be provided to Data Providers for review.

- Based on the results of the Risk Assessment and recommendations from Data Providers, the System Steward shall apply additional constraints as necessary to the usage of the Linked Data.
- These constraints shall, at a minimum, include:
    a. The Data Consumer must destroy the Linked Data after 6 months of receipt (or less if the risk is determined to be high), with accompanying proof of destruction submitted to System Steward. The maintenance of a de-identified data file is appropriate given the established permission of the providing agency;
    b. The System Steward must follow up after specified time period to review results of data usage by Data Consumer; and
    Data Consumer must confirm, to the Data's Consumer's best knowledge, that no PII was released to additional third parties.
- Final agreement on additional constraints shall be documented in the use case in the attached appendix, and signed by the Providers, the Requestors and System Steward as appropriate, *prior to* release of Linked Data.

X. *Data Accuracy*

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

XI. Confidentiality

A. The Data Consumer shall protect Data and information according to acceptable standards and no less rigorously than it protects its own confidential information. Personal Identifying Information will not be reported or made public.

B. To the extent applicable, all Data sharing shall be performed in accordance with the requirements of HIPAA. HIPAA Section 164.514(a)-(c) provides that de-identified personal health information may be released without the individual's specific written permission when "(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements; (1) An adequate plan to protect the identifiers from improper use and disclosure; (2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and (3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart; (B) The research could not practicably be conducted without the waiver or alteration; and (C) The research could not practicably be conducted without access to and use of the protected heath information." Additional provisions existing in C.F.R. Title 45, Parts 160, 162, and 164 shall be complied with as they apply to this agreement.

C. Additionally, CDE shall comply with any agency- or program-specific requirements outlined in C.R.S. Title 22 and corresponding regulations, and CDPS shall comply with any agency- or program-specific requirements outlined in CDPS Administrative Regulations as well as any corresponding regulations, that govern the sharing of protected information.

XII. Non-Financial Understanding

This Agreement is a non-financial understanding between the Parties. 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. 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. 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.

XIII. Data Retention

A. Data Consumers agree to securely maintain Data while conducting the research specified in the Agreement. All unnecessary records shall be purged within 6 months from the time it was released to the Data Consumer, or sooner if the data has already served the purpose specified in the use case in the attached appendix. Records shall either be returned to the Data Provider or destroyed in a secure manner. Data retention policies shall comply with the Colorado State Archives Records Management Manual for State Government Agencies http://www.colorado.gov/dpa/doit/archives/rm/rmman/index.htm. After data is destroyed, the Data Consumer shall provide written confirmation to the Data Provider.

B. Any external party housing Data on behalf of one of the parties agrees to the same standards, restrictions, and conditions of this Agreement.

XIV. Data Governance Plans

CDPS is governed by the Governor's Office of Information Technology's cyber security policy. This policy represents the data governance plan. Both Parties agree to have in place a Data Governance plan with support and participation from across their organizations that detail the organization's policies and procedures to protect privacy and data security, including ongoing management of data collection, processing, storage, maintenance, use and destruction. Each Party has the right to conduct audits or other monitoring activities of the other Party's Data Governance policies, procedures, and systems. If, through these monitoring activities, vulnerability is found, the breaching Party must take timely appropriate action to correct or mitigate any weaknesses discovered.

XV. Unauthorized Uses, Disclosures or Breaches

A. In the event a Data Breach occurs as a result of Data sharing, the Data Consumer shall be responsible for notifying the Data Provider and working with the respective agencies' Data Governance Managers (or delegates as noted in the appropriate appendix) in contacting and informing the individual students or parties who may have been affected by the Data Breach. Data Consumers may not contact individual students or parties prior to notification of the Data Provider.

B. Should a person not comply with this agreement, he/she may be subject to disciplinary action, including, but not limited to, termination of access authorization.

C. Failure to comply with this policy may result in denial of access or any actions deemed "inappropriate dissemination of student or staff data" may result in a penalty as defined in section 6-1-716 of Colorado Revised Statutes.

D. CDE and CDPS shall make a good faith effort to identify any use or disclosure of confidential Data not authorized by this agreement.

E. If there are costs associated with notifying individuals whose personally identifiable information has been compromised or any other damages resulting from the release of the Data, the compensating party shall depend on determined fault for the initial Data breach. If the Data Provider is responsible for the breach, the Data Provider shall compensate for communication and damages. If the Data Consumer is responsible for the breach, the Data Consumer shall compensate for communication and damages.

XVI. Survival

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

XVIII. Effective Date and Term

This Agreement shall take effect upon its signing by all parties. This Agreement may be amended at any time by mutual agreement of all parties. All parties will conduct an independent review of this Agreement on an annual basis. This Agreement shall remain in effect until terminated by written notification from one party to another.

XIX. Signatures

To further the collection and analysis of Colorado educational data, CDE, represented by the Commissioner of Education for Colorado, Robert Hammond, and CDPS, represented by Deputy Executive Director CDPS, Kathy Sasak, agree to the cooperative sharing of data between the two agencies pursuant to the conditions set forth herein.

Signature: _____ *Date:* 11/10/14

Robert Hammond
Commissioner of Education
Colorado Department of Education

Signature: _____ *Date:* 11/12/14

Kathy E. Sasak
Deputy Executive Director
Colorado Department of Public Safety

APPENDIX A – CDE – CDPS Use Case

Business Use Case - Purpose

The purpose of the data sharing agreement is to support a study sponsored by the Division Criminal Justice within CDPS to determine whether detention as a sanction for truancy had any positive or negative impacts on youth adjudicated truant. The design of the study requires the integration of individual level data from multiple state agencies including the CDPS Division of Criminal Justice and CDE. Utilizing data from four state agencies, we will examine preceding characteristics and events that may have influenced whether youth adjudicated truant received a detention sentence and will also examine subsequent outcomes for youth who received a truancy related detention sentence and for youth adjudicated truant who did not receive a detention sentence.

Participating Agencies

The **Colorado Department of Education** (CDE) will be sharing data with the **Colorado Department of Public Safety** (CDPS)

Data Required from CDE – Data Provider

- Last name
- First Name
- Date of Birth
- Gender
- Race/Ethnicity
- School Year
- Type of school (public vs facility)
- School
- Free or reduced lunch eligibility
- Enrollment status
- Leave date
- Exit Code
- Grade retention
- SE designation
- IEP (Yes/No)
- Primary language
- Language Proficiency Status
- Language Program Participation (e.g., ESL, bilingual, etc)
- Masked EASID

Data Required from CDPS – Data Provider

CDPS will provide information on the youth to match to CDE files. The following variables will be included to narrow the relevant records:

a. Last Name

b. Date of Birth

c. Gender

d. Ethnicity

Duration of Study (specify how long data will be required)

The data sharing described within this use case will be ongoing until CDE and or CDPS decide to terminate the process. The agreement will be reviewed, updated and approved on an annual basis.

Conditions under which data may and may not be linked and shared

Data will be linked via the student demographic information and all data analysis will be conducted by the CDPS evaluation unit and/or their contracted agencies. The System Steward for this Use Case/Appendix shall be CDPS.

For the purpose of the above business use case, the roles of data consumer and authorized user shall be limited to the below identified data owners and data consumers. CDE and CDPS may identify additional staff as authorized users in writing for review and consideration.

CDPS includes as data consumers:

- Meg Williams: Division of Criminal Justice, Department of Public Safety.
- Tara Wass: Center for Research Strategies and PI of the study.
- Diane Fox: Center for Research Strategies and Co-PI of the study.

The role of Data Governance Manager for CDE is Marcia Bohannon for this agreement, and the role of Data Governance Manager for CDPS is Kim English in conjunction with the below outlined interim data governance process. After the establishment of a formal Data Governance Manager at CDPS, that staff will assume the responsibilities outlined in the definitions section and in accordance with roles and responsibilities as assigned by CDPS.

Table of Required Data and Ownership:

Data	From	Source System	Data Owner
1. Public School (K-12)	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
2. Truancy	CDPS	CJASS	Kim English, DCJ Research Director Peg Flick, DCJ Senior Analyst

CDPS Processes

CDPS, in order to facilitate the data sharing outlined in this Appendix and comply with the practices outlined in the Agreement asserts that all activities regarding data storage, handling, sharing, disclosure or other activities will comply with the cyber security policy detailed by the Governor's Office of Information Technology.

Regulations that Apply

- FERPA

Additional Constraints, as required by Section VIII, entitled "Release of Linked Data to Requestor"

Signatures

To further the collection and analysis of Colorado educational Data, CDE, represented by CDE's Data Governance Manager, Jan Rose Petro, RISE Data Governance Manager, Marcia Bohannon, and the Commissioner of Education, and from CDPS the Deputy Executive Director, Kathy Sasak and the Director of Research, Kim English.

Signature: _____ *Date:* 11/10/14

Robert Hammond
Colorado Commissioner of Education
Colorado Department of Education

Signature: Jan Rose Petro *Date:* 11/10/14

Jan Rose Petro
Director, Data Services Unit
Colorado Department of Education

Signature: Marcia Bohannon *Date:* 11/7/14

Marcia Bohannon
Deputy Chief Information Officer
Colorado Department of Education

Signature: _____ *Date:* 11/6/14

Kathy E Sasak
Deputy Executive Director
Colorado Department of Public Safety

Signature: Kim English *Date:* 11/5/14

Kim English
Director of Research
Colorado Department of Public Safety
Division of Criminal Justice