

**MEMORANDUM OF UNDERSTANDING
(INFORMATION SHARING AGREEMENT)
BY AND BETWEEN
THE UTAH DEPARTMENT OF HUMAN SERVICES,
THE UTAH STATE OFFICE OF EDUCATION,
AND THE UTAH JUVENILE COURT**

Effective from July 1, 2021 through June 30, 2026

- A. Parties: This agreement is between the Utah Department of Human Services (DHS), the Utah State Board of Education (USBE), and the Utah Juvenile Court.
- B. Purpose: This Memorandum of Understanding (MOU) authorizes the exchange of education and human services data to enable all parties to improve educational outcomes for youth served by DHS programs, the Utah Juvenile Court, and/or students receiving Youth in Custody (YIC) services.
- C. Legal Authority:
1. Federal laws
 - i. Family Educational Rights and Privacy Act (FERPA) – 20 U.S.C. § 1232g grants DHS custodial agencies (including case workers, case managers, or foster parents who serve as the legal custodian and/or guardian of a child who is a student) the authority to inspect and review education records for youth served.
 - ii. Uninterrupted Scholars Act (USA) – Public Law 112-278, an amendment to 20 U.S.C. § 1232g, authorizes access of the Utah Juvenile Court to educational records for youth in proceedings involving child abuse and neglect or dependency matters.
 - iii. Individuals with Disabilities Education Act (IDEA) 20 U.S.C. § 1417(c) ensures the protection of the confidentiality of any personally identifiable data, information, and records collected or maintained by the state educational agencies. The IDEA makes available a free appropriate public education to eligible children with disabilities and ensures special education and related services to those children through an individualized education program (IEP).
 - iv. Section 504 of the Rehabilitation Act of 1973 (Section 504), 20 U.S.C. § 794 prohibits discrimination on the basis of disability, including the exclusion of participation in or denial of the benefits of any program or activity receiving federal financial assistance. Accommodations for qualified students are documented in a 504 plan.
 2. State laws
 - i. Public Education System – State Administration, Student Privacy and Data Protection, Utah Code Annotated § 53E-9-308(3) and (4). This law grants authority to the Department of Human Services to receive student specific data and cites additional authority in Utah Code § 62A-4a-409(5), Investigation by division -- Temporary protective custody – Pre-removal interviews of children.
 - ii. Education of individuals in custody of or receiving services from certain state agencies -- Establishment of coordinating council -- Advisory councils, Utah Code Annotated § 53E-3-503. This law directs the state board to expend funds for the education of youth in custody.
 - iii. Government Records Access and Management Act (GRAMA) – By entering into this MOU, each of the parties hereby provides written agreement that the records that shared, viewed, and

used will only be shared, viewed and used in compliance with Utah Code Annotated § 63G-2-206(2), the GRAMA permits private, protected, or controlled records to be provided to another governmental entity if it is necessary to the performance of that entity's duties and functions, will be used for a purpose similar to the purpose for which the information in the record was collected, and the public benefit outweighs the individual privacy right that protects the record.

D. Access to Data:

1. Access by DHS and the Utah Juvenile Court to information gathered and/or administered by USBE:
 - i. If the information concerns a student in the custody of or is receiving services through DHS, the DHS employee with legitimate education interest is entitled to education records and/or personally identifiable information about a student without parental consent. A "caseworker or other representative of a State or local child welfare agency" is authorized to access a "student's case plan," as defined in 20 U.S.C. § 1232g(b)(1)(L).
 - ii. DHS divisions, offices, and institutions are authorized to share educational records within the department for youth in the custody of a DHS division, and those under the jurisdiction of the Utah Juvenile Court through system interfaces that meet the data security provisions outlined below.
 - iii. If a student is under the jurisdiction of the Utah Juvenile Court, DHS may share education records and/or personally identifiable Information about a student with a Utah Juvenile Court employee engaged in addressing the student's education needs.
 - iv. DHS divisions, offices, and institutions receiving student records will not redisclose education records to third parties except as expressly provided under the law.
 - v. USBE shall redact student records that contain information about students who are not the subject of the records requested by DHS as required by law.
 - vi. USBE shall provide DHS with data elements that include:
 - 1) Statewide Student Identifier (SSID)
 - 2) School Year
 - 3) Local education authority (LEA) name
 - 4) LEA identifier
 - 5) School name
 - 6) School identifier and/or school number
 - 7) School type
 - 8) Grade level
 - 9) Entry date
 - 10) Exit date
 - 11) English language learner (ELL) status
 - 12) Race
 - 13) Special education indicator
 - 14) Low-income indicator
 - 15) Youth in Custody (YIC) indicator
 - 16) Percent absent
 - 17) Days enrolled
 - 18) Percent attendance
 - 19) Chronically absent indicator
 - 20) Cumulative grade-point average (GPA)

- 21) October 1 enrollment indicator
 - 22) High school completion status
 - 23) Final high school status
 - 24) Course title
 - 25) Course core code
 - 26) Grade
 - 27) Course section
 - 28) Credits attempted
 - 29) Credits earned
 - 30) Test subject area
 - 31) Test subject identifier
 - 32) Test name
 - 33) Proficiency level
 - 34) Scale score
 - 35) Student growth percentile (SGP)
 - 36) Proficiency indicator
 - 37) Tested below grade level indicator
 - 38) Proficiency level description
- vii. This data shall include data for the most recent 10 years as available.
2. Access by DHS and the Utah Juvenile Court to information gathered and/or administered by the local education authority (LEA):
- i. Pursuant to this agreement, when a student is in the custody of a division of DHS or receiving services through a division of DHS, each LEA or school shall provide a DHS employee or designee, and/or Utah Juvenile Court employee, with the same education record that would be provided to a parent. This includes those records, files, documents, and other materials which contain information directly related to a student and are maintained in an educational agency or institution or by a person acting for such agency or institution (20 U.S.C. § 1232g(a)(4)(A)).
 - ii. Furthermore, each school shall provide copies of a student's education record to the DHS designee or Utah juvenile Court employee upon written or electronic request accompanied by appropriate identification of the employee requesting the Information. To the extent that the records can be shared electronically, this MOU contemplates electronic record sharing, digital, and telephonic communications record sharing using secure data transfer and encryption as described in paragraph F.
 - iii. LEAs shall provide access to DHS divisions regarding data elements that include all those listed in paragraph D.1.(vi) above plus IEP/504 eligibility status and plan, disciplinary action, and the number of school placements.
 - iv. Requested education records shall be provided to a DHS division caseworker, or designee, as soon possible, upon receipt of an appropriate request and the provision of appropriate identification.
 - v. LEAs shall redact information in student records that pertain to students who are not the subject of the records requested by DHS as required by law.
3. Access by USBE and LEAs to information gathered and/or administered by DHS for Youth in Custody coordination:
- i. Pursuant to this agreement, DHS shall provide to USBE electronic or hard copy data in its possession for youth in the custody of a division of DHS, as needed for school enrollment. DHS

shall provide additional data elements when requested and if available. Data elements include the following:

- 1) Student Name
 - 2) Caseworker/Manager Name
 - 3) Caseworker/Manager Contact Information
 - 4) Student Demographic Information including
 - 5) Date of Birth
 - 6) Current Grade
 - 7) Gender
 - 8) Ethnicity
 - 9) Placement and placement contact information
 - 10) Previous school enrollments
 - 11) Additional known information including special education status, English Language Learner status, safe school violations, current school safety plans
 - 12) Previous DHS services
 - 13) Immunization Record
 - 14) Known social/medical information
 - 15) Permanency plans
 - 16) UFACET or other internal assessment for the purpose of engagement
 - 17) Education relevant summary information from psychological evaluation
- ii. Likewise, DHS shall provide timely information to schools/LEAs in support of eligible DHS youth in care to meet the educational needs of the custodial school age population and to maintain a safe school environment for all students.

E. Data Transfer:

1. Electronic data may be transferred in the following ways:
 - i. Through interfaces where the data is encrypted in transit and the connection is secure.
 - ii. To a specific individual using a secure and encrypted FTP site that is password protected.
2. Paper copies will only be given to individuals who show proper state-issued identification such as an ID badge with picture issued by one of the parties to this MOU.

F. Data Security:

1. In addition to the requirements below, all parties agree to the provisions in the addendum for definitions, access to data, use and disclosure of data, security and protection of data, and incidents.
2. All shared data will be stored in a password protected database or network location with encrypted drives and/or in the drives of password protected and encrypted workstations.
3. Paper and electronic files will be stored in a physically secure location. A physically secure location is a facility, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the data and associated information systems in question.
4. Only persons with proper authorization will be allowed to access shared data.
5. Educational records will not be re-disclosed and will not be used for any other purpose other than to improve educational stability unless there is a court order to do so. Additionally, this MOU relies on Utah Code Annotated § 63G-2-206(2) Government Records Access and Management Act

(GRAMA) permitting private, protected, or controlled records to be provided to another governmental entity if the requesting entity provides written assurance if it is necessary to the performance of that entity's duties and functions, will be used for a purpose similar to the purpose for which the information in the record was collected, and the public benefit outweighs the individual privacy right that protects the record.

G. Termination: This MOU is effective upon the signature of all parties and shall continue until the due date unless modified in writing by the mutual consent of all parties or terminated by any party upon 30 days prior written notice to the other parties by certified or registered mail, return receipt requested. Any agency may terminate this MOU without prior notice if deemed necessary because of a requirement of law or policy, upon determination that there has been a breach of system integrity or security, or failure to comply with established procedures or legal requirements. In the event of termination, data in possession of the respective parties may be retained only as necessary to fulfill legitimate education interests. Data shared under the authority of this MOU is perpetually subject to the data security and privacy protections described in the Addendum even if the MOU is terminated.

H. Points of Contact

DHS
Rick Little, Director
Management Information Center
Department of Human Services
ricklittle@utah.gov

USBE
Whitney Phillips or
David Sallay
Information Technology
Utah State Board of Education
whitney.phillips@schools.utah.gov
david.sallay@schools.utah.gov

Utah Juvenile Court
Zerina Ocanovic,
Research Analyst
Administrative Office of the Courts
zerinao@utcourts.gov

I. APPROVALS:

Tracy Gruber, JD
Interim Executive Director
Utah Department of Human Services
801-538-4001


Tracy Gruber (Aug 31, 2021 05:33 MDT) Date 08/31/2021
Signature _____

Dr. Whitney Phillips
Chief Privacy Officer
Utah State Board of Education
801-538-7523

Date _____
Signature _____

Ron Gordon, JD
State Court Administrator
Utah Administrative Office of the Courts
801-578-3816


Date 8/27/21
Signature _____

Aaron Brough
Data and Statistics Coordinator
Utah State Board of Education
801-538-7922

Date _____
Signature _____

ADDENDUM: STANDARD TERMS AND CONDITIONS FOR DATA USE

The following provisions are hereby addended to the Memorandum of Understanding (MOU) by and between the Utah Department of Human Services (DHS), the Utah State Board of Education (USBE), and the Utah Juvenile Court. The definitions of terms used in this Addendum are as set forth in Section 1 below, and the Definitions in Section 1 below shall apply only to this Addendum.

These terms and conditions protect data subject to the provisions of the Family Educational Rights and Privacy Act (FERPA). As referred in this Addendum, USBE is the "principal" of data protected by FERPA and DHS and the Juvenile Courts are the "partners."

1. **DEFINITIONS:** The following terms shall have the meanings set forth below:
 - 1.1. "**Authorized Persons**" means Partner's employees, officers, divisions other agents of Partners who require access to Data and who have a legitimate educational interest in the education records to enable the Partners to perform their responsibilities under this MOU.
 - 1.2. "**Confidential Information**" means information that is deemed as confidential under applicable state and federal laws. The Principal reserves the right to identify, during and after this MOU, additional reasonable types of categories of information that must be kept confidential under federal and state laws.
 - 1.3. Memorandum of Understanding (MOU) means the agreement including the signature page(s), all referenced attachments and documents incorporated by reference.
 - 1.4. "**MOU Signature Page(s)**" means the page(s) in the MOU that the Principle and Partners signed.
 - 1.5. "**Partners**" are the agencies receiving USBE data as identified in the MOU. The term "Partner" shall include Partners' agents, officers, and employees.
 - 1.6. "**Data**" includes Student Personally Identifiable Information and Educator Data, and may also include Confidential Information.
 - 1.7. "**Destroy**" means to remove Data such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.
 - 1.8. "**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.
 - 1.9. "**Incident**" means the potentially unauthorized access to Data that the Principal believes could reasonably result in the use, disclosure or theft of Data within the possession or control of the Partners.
 - 1.10. "**Metadata**" includes all information created manually or automatically to provide meaning or context to other data.
 - 1.11. "**Partner**" means the Department of Human Services or the Juvenile Courts including all subordinate divisions, offices, bureaus, agencies, or other organizations identified on the MOU Signature Page(s).
 - 1.12. "**Principal**" means the State Board of Education, in its entirety, including its institutions, agencies, departments, divisions, authorities, instrumentalities, boards, commissions, elected or appointed officers, employees, agents, and authorized volunteers.
 - 1.13. "**Student Personally Identifiable Information**" or "**PII**" has the same meaning as that found in U.C.A § 53E-9-301, and includes both direct identifiers (such as a student's or other family member's name, address, student number, or biometric number) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name). Indirect identifiers that constitute PII also include metadata or 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.
2. **ACCESS TO DATA:**
 - 2.1. Partners shall limit access to Data to Authorized Persons only and shall require a non-disclosure agreement be signed by all Authorized Persons prior to being granted access to Data.
 - 2.2. Partners shall maintain past and current lists of all Authorized Persons, maintain each non-disclosure agreement, and shall permit inspection of the same by USBE upon request.
 - 2.3. Partners shall maintain an audit trail for the duration of this MOU, which reflects the granting and revoking of access privileges to Authorized Persons. A copy of this audit trail may be requested by USBE from Partners at any time and shall be provided within 10 days of the USBE request.
 - 2.4. Partners shall have strong access controls in place. Partners shall disable and/or immediately delete unused and terminated Authorized Persons' accounts and shall periodically assess account inactivity for potential stale accounts.
 - 2.5. Partners shall provide annual, mandatory privacy and security awareness and training for all Authorized Persons, maintain past and current lists of Authorized Persons that have completed training, and permit inspection of the same by USBE upon request.

3. USE AND DISCLOSURE OF DATA:

- 3.1. Partners shall not collect, use, or share Data beyond the purposes set forth as follows:
 - 3.1.1. To carry out the Partners responsibilities as defined in the MOU.
- 3.2. Partners shall share data only for the purposes stated in paragraph B of this MOU and the following entities:
 - 3.2.1. The parties to this MOU.
 - 3.2.2. Law enforcement agencies or individuals only as authorized by law or court order. Contractor receives such a request, Partners shall notify USBE within two (2) business days of the receipt of the request, as permitted by law.
- 3.3. If Partners seek to publicly release Data, Partners must aggregate the Data by totaling the Data and reporting it at the group, cohort, school, school district, region, or state level. Partners shall, upon request of USBE, provide USBE with a document that lists the steps and methods the Partner shall use to de-identify the information. Any aggregate data that is publicly released without being redacted using the methods in this section shall be considered an Incident. The following methods shall be used on any aggregated reports:
 - 3.3.1. Aggregate data shall be reported publicly only if there is a sufficient number of individuals represented in any demographic or subgroup so that an individual cannot be identified.
 - 3.3.2. Aggregated reports shall be redacted using complementary suppression methods that remove the risk of Data being identifiable using simple mathematics or formulas.
 - 3.3.3. Aggregated reports shall be redacted to remove identifiability risks caused other prior releases of aggregate data by Partners.
- 3.4. Partners shall not use Data for the purposes of Targeted Advertising except under the following conditions:
 - 3.4.1. For adaptive learning or customized student learning purposes.
 - 3.4.2. To market an educational application or product/service to a parent or legal guardian of a student if Partner did not use Data, shared by or collected per this MOU, to market the educational application or product/service.
 - 3.4.3. To use a recommendation engine to recommend to a student (i) content that relates to learning or employment, within the third-party partner's internal application, if the recommendation is not motivated by payment or other consideration from another party; or (ii) services that relate to learning or employment, within the third-party partner's internal application, if the recommendation is not motivated by payment or other consideration from another party;
 - 3.4.4. To respond to a student request for information or feedback, if the content of the response is not motivated by payment or other consideration from another party.
 - 3.4.5. To use Data to allow or improve operability and functionality of the third-party partner's internal application.
- 3.5. Partners shall not sell or otherwise monetize Data except Data transferred through the purchase of, merger with, or otherwise acquisition of Partners provided that all parties remain in compliance with this MOU.

4. SECURITY AND PROTECTION OF DATA:

- 4.1. Partners shall notify USBE of material system changes that may negatively impact the security of Data prior to such changes being implemented.
- 4.2. If Partners are given Data as part of this MOU, the protection of Data shall be an integral part of the business activities of Partners to ensure that there is no inappropriate or unauthorized use of Data. Partners shall safeguard the confidentiality, integrity, and availability of Data.
- 4.3. Partners shall comply with and protect and maintain Data using methods that are at least as good as or better than that established in the State of Utah's Department of Technology Policies (<https://dts.utah.gov/policies>).
- 4.4. Partners shall only transmit or exchange Data via secure means (ex. HTTPS or FTPS). Contractor shall not use, store or process Data on any unencrypted portable or laptop computing device or any portable storage medium.
- 4.5. Partners shall store and maintain all Data in data centers located in the United States.
- 4.6. Partners shall permit its employees and Subcontractors to access Data remotely only via a secured manner, such as Virtual Private Networks (VPN).
- 4.7. Partners shall store all Data, as well as any backups made of that data, in encrypted form using no less than 128-bit key and include all Data as part of a designated backup and recovery process.
- 4.8. Partners shall enforce strong password protections on all devices and networks with access to or that store Data.

5. INCIDENTS:

- 5.1.** If a Partner becomes aware of an Incident involving Data by either Partner or any of division, Partners shall notify USBE within one (1) calendar day and cooperate with USBE regarding recovery, remediation, and the necessity to involve law enforcement, if any.
- 5.2.** Partners shall produce a written remediation plan that includes information about the cause and extent of the Incident and the actions Partners will take to remediate the Incident and to reduce the risk of incurring a similar type of Incident in the future. Partners shall present their analysis and remediation plan to USBE within ten (10) calendar days of notifying USBE of an Incident. USBE reserves the right to adjust this plan, in its sole discretion. If Partners cannot produce its analysis and plan within the allotted time, USBE, in its sole discretion, may perform such analysis and produce a remediation plan, and Partners shall reimburse USBE for the reasonable costs thereof.
- 5.3.** In the event of an Incident, Partners shall provide USBE 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.
- 5.4.** Unless Partners can establish that they or any of their divisions are not the cause or source of the Incident, Partners shall be responsible for the cost of notifying each person whose personal information may have been compromised by the Incident.
- 5.5.** Disclosure of Data by Partners or any division for any reason not authorized in this MOU may be cause for legal action by third parties against Contractor, the State, or their respective agents. Contractor shall indemnify, save, and hold harmless the State, its employees, and agents against any and all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred as a result of any act or omission by Partners, or its employees, agents, divisions, or assignees pursuant to this MOU. Notwithstanding any other provision of this Contract, Partners shall be liable to the State for all direct, consequential, and incidental damages arising from an Incident caused by Partners or their divisions.