Emery County School District

Policy: EH—Data Governance

Date Adopted: 9 August 2017
Current Review / Revision: 9 August 2017

Table of Contents

Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data, from acquisition, to use, to disposal. The Utah Board of Education and Emery School District take seriously the moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-301 requires that Emery School District adopt a Data Governance Plan.

Scope & Applicability

This policy is applicable to all employees, temporary employees, and contractors of the Agency. The policy must be used to assess agreements made to disclose data to third-parties. This policy must also be used to assess the risk of conducting business. In accordance with Agency policy and procedures, this policy will be reviewed and adjusted on an annual basis or more frequently, as needed. This policy is designed to ensure only authorized disclosure of confidential information. The following 8 subsections provide data governance policies and processes for Emery School District:

- Data Advisory Groups
- Non-Disclosure Assurances for Employees
- Data Security and Privacy Training for Employees
- Data Disclosure
- Data Breach
- Record Retention and Expungement
- Data Quality
- Transparency

Furthermore, this Emery School District Data Governance Plan works in conjunction with the Agency Information Security Policy, which:

- Designates the current Director of Technology and Director of Student Services as the stewards for all confidential information maintained within Emery School District.
- Designates Data Stewards access for all confidential information.
- Requires Data Stewards to maintain a record of all confidential information.
- Requires Data Stewards to manage confidential information according to this policy and all other applicable policies, standards and plans.
- Complies with all legal, regulatory, and contractual obligations regarding privacy of Agency data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence.
- Provides the authority to design, implement, and maintain privacy procedures meeting Emery School District standards concerning the privacy of data in motion, at rest and processed by related information systems.
- Ensures that all Emery School District board members, employees, contractors, and volunteers comply with the policy and undergo annual privacy training.
- Provides policies and process for:
    - Systems administration,
    - Network security,
    - Application security,
    - Endpoint, server, and device security
    - Identity, authentication, and access management,
    - Data protection and cryptography
    - Monitoring, vulnerability, and patch management
    - High availability, disaster recovery, and physical protection

- Incident responses
- Acquisition and asset management, and
- Policy, audit, e-discovery, and training.

Data Advisory Groups

Structure: Emery School District has a three-tiered data governance structure to ensure that data is protected at all levels of Utah's educational system.

Group Membership: Membership in the groups require board approval. Group membership is for two years. If individual members exit the group prior to fulfilling their two-year appointment, the board may authorize Emery School District's Chief Officer to appoint a replacement member.

Individual and Group Responsibilities

LEA Student Data Managers

- Authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity
- Act as the primary local point of contact for the state student data officer.
- A student data manager may share personally identifiable student data that are:
  - of a student with the student and the student's parent
  - required by state or federal law
  - in an aggregate form with appropriate data removal techniques applied
  - for a school official
  - for an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court
  - in response to a subpoena issued by a court
  - directory information
  - submitted data requests from external researchers or evaluators
- A student data manager may not share personally identifiable student data for the purpose of external research or evaluation.
- Create and maintain a list of all LEA staff that have access to personally identifiable student data.
- Ensure annual LEA level training on data privacy to all staff members, including volunteers. Document all staff names, roles, and training dates, times, locations, and agendas.

IT Systems Security Manager

- Acts as the primary point of contact for state student data security administration
- Ensures compliance with security systems laws throughout the public education system, including providing training and support to applicable Emery School District employees
- Investigates complaints of alleged violations of systems breaches
- Provides an annual report to the board on Emery School District's systems security needs

Employee Non-Disclosure Assurances

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information.

Scope: All Emery School District board members, employees, contractors and volunteers must sign and obey the Emery School District Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of state technology and information.

Non-Compliance: Non-compliance with the agreements shall result in consequences up to and including removal of access to the Emery School District network; if this access is required for employment, employees and contractors may be subject to dismissal.

Non-Disclosure Assurances: All student data utilized by Emery School District is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way Emery School District staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all Emery School District staff to verify agreement to adhere to/abide by these practices and will be maintained in Emery School District. All Emery School District employees (including contract or temporary) will:

- Complete a Security and Privacy Fundamentals Training.
- Consult with Emery School District internal data owners when creating or disseminating reports with data.
- Use password-protected state-authorized computers when accessing any student-level or staff-level records.
- NOT share individual passwords for personal computers or data systems with anyone.
- Log out of any data system/portal and close the browser after each use.
- Store sensitive data on appropriate-secured locations. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
- Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at Emery School District when disposing of such records.
- NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used for such presentations.
- Remove any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager, found in Appendix B (Protecting PII in Public Reporting).
- Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
- Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
- NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy Manager should be consulted.
- Use secure methods when sharing or transmitting sensitive data.
- NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods such as described in item ten.
- Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

Data Security and Privacy Training

Purpose: Emery School District will provide a range of training opportunities for all District staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.

Scope: All District board members, employees, and contracted partners.

Compliance: New employees that do not comply may not be able to use District networks or technology.

Policy

- Within the first week of employment, all Emery School District board members, employees, and contracted partners must sign and follow the Emery School District Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.

- Employees that do not comply may not be able to use Emery School District networks or technology. Within the first week of employment, all new Emery School District board members, employees, and contracted partners also must sign and obey the Emery School District Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.

- All current Emery School District board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 60 days of the adoption of this rule.

- Emery School District requires a targeted Security and Privacy Training for Data Stewards and IT staff or other specific groups within the agency that collect, store, or disclose data. The Chief Privacy Officer will identify these groups. Data and Statistics Coordinator will determine the annual training topics for these targeted groups based on Emery School District training needs.

- Participation in the training as well as a signed copy of the Employee Non-Disclosure Agreement will be annually monitored by supervisors. Supervisors and the board secretary will annually report all Emery School District board members, employees, and contracted partners who do not have these requirements completed to the IT Security Manager.

Data Disclosure

Purpose: Providing data to persons and entities outside of the Emery School District increases transparency, promotes education in Utah, and increases knowledge about Utah public education. This policy establishes the protocols and procedures for sharing data maintained by Emery School District. It is intended to be consistent with the disclosure provisions of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 CFR Part 99 and Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-301.

Policy for disclosure of Personally Identifiable Information (PII)

- Student or Student's Parent/Guardian Access: Parents are advised that the records maintained by Emery School District are provided to Emery School District by the school district in which their student is/was enrolled, and access to their student's record can be obtained from the student's school district. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), LEAs will provide parents with access to their child's education records, or an eligible student access to his or her own education records (excluding information on other students, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access), within 45 days of receiving an official request. Emery School District is not required to provide data that it does not maintain, nor is Emery School District required to create education records in response to an eligible student's request.

- Third Party Vendor: Third party vendors may have access to students' personally identifiable information if the vendor is designated as a "school official" as defined in FERPA, 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii). A school official may include parties such as: professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor, consultant, volunteer or other party to whom the school has outsourced institutional services or functions.
- All third-party vendors contracting with Emery School District must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-301. Vendors determined not to be compliant may not be allowed to enter into future contracts with Emery School District without third-party verification that they are compliant with federal and state law, and board rule.
- Internal Partner Requests: Internal partners to Emery School District include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in Emery School District's data request ticketing system.
- The Coordinator of Data and Statistics will ensure the proper data disclosure avoidance are included if necessary. An Interagency Agreement must be reviewed by legal staff and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."
- Governmental Agency Requests: Emery School District may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program reporting requirement, audit, or evaluation. The requesting governmental agency must provide evidence the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions to data without consent in the case of a federal or state:
    - reporting requirement
    - audit
    - evaluation

The Coordinator of Data and Statistics will ensure the proper data disclosure avoidance are included if necessary. An Interagency Agreement must be reviewed by legal staff and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."

External Disclosure of Non-Personally Identifiable Information (PII)

Scope: External data requests from individuals or organizations that are not intending on conducting external research or are not fulfilling a state or federal reporting requirement, audit, or evaluation.

Student Data Disclosure Risk Levels: Emery School District has determined three levels of data requests with corresponding policies and procedures for appropriately protecting data based on risk: Low, Medium, and High. The Coordinator of Data and Statistics will make final determinations on classification of student data requests risk level.

Low-Risk Data Request Process

- Definition: High-level aggregate data
- Examples: Graduation rate by year for the state; Percent of third-graders scoring proficient on the SAGE ELA assessment
- Process: Requester creates a ticket and Data Request is forwarded to appropriate Data Steward. Data Steward fulfills request and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket.

Medium-Risk Data Request Process

- Definition: Aggregate data, but because of potentially low n-sizes, the data must have disclosure avoidance methods applied
- Examples: Graduation rate by year and LEA; Percent of third-graders scoring proficient on the SAGE ELA assessment by school; Child Nutrition Program Free or Reduced Lunch percentages by school
- Process: Requester creates a ticket and Data Request is forwarded to appropriate Data Steward, Data Steward fulfills request, applies appropriate disclosure avoidance techniques, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.

High-Risk Data Request Process

- Definition: Student-level data that are pre-identified.
- Examples: Pre-identified student-level graduation data; Pre-identified student-level SAGE ELA assessment scores for grades 3-6.
- Process: Requester creates a ticket and Data Request is forwarded to Data and Statistics Coordinator for review. If the request is approved, an MOA is drafted and sent to legal, placed on the board consent calendar, reviewed by the Superintendent, sent to the Purchasing/Contract Manager, sent to Coordinator or Data and Statistics, appropriate Data Steward fulfills request, de-identifies data as appropriate, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.

Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The Coordinator of Data and Statistics will ensure the proper data are shared with external researcher or evaluator to comply with federal, state, and board rules.

Emery School District may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program audit or evaluation. Data that do not disclose PII may be shared with external researcher or evaluators for projects unrelated to federal or state requirements if:

- An Emery School District Director, Superintendent, or board member sponsors an external researcher or evaluator request.
- Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Coordinator of Data and Statistics.
- Researchers and evaluators supply the Emery School District a copy of any publication or presentation that uses Emery School District data 10 business days prior to any publication or presentation.

Process: Research Proposal must be submitted using this form: http://www.schools.utah.gov/data/Data-Request/ResearcherProposal.aspx. Research proposals are sent directly to the Coordinator of Data and Statistics for review. If the request is approved, an MOA is drafted and sent to legal, placed on the board consent calendar, reviewed by the Superintendent, sent to the Purchasing/Contract Manager, sent to Coordinator or Data and Statistics, appropriate Data Steward fulfills request, de-identifies data as appropriate, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.

Data Breach

Purpose: Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination and help educational organizations shorten their incident response time. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals.

Policy: Emery School District shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, Emery School District staff shall follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, Emery School District shall follow best practices for notifying affected parties, including students, in the case of an adult student, or parents or legal guardians, if the student is not an adult student.

Concerns about security breaches must be reported immediately to the IT security manager who will collaborate with appropriate members of the Emery School District executive team to determine whether a security breach has occurred. If the Emery School District data breach response team determines that one or more employees or contracted partners have substantially failed to comply with Emery School District's Agency IT Security Policy and relevant privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action. Concerns about security breaches that involve the IT Security Manager must be reported immediately to the Superintendent.

Emery School District will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach. Emery School District will make these resources available on its website.

Records Retention and Expungement

Purpose: Records retention and expungement policies promote efficient management of records, preservation of records of enduring value, quality access to public information, and data privacy.

Scope: Emery School District board members and staff.

Policy: The Emery School District staff, Utah LEAs and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53E-9-301, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with 53E-9-301, the Emery School District shall expunge student data that is stored upon request of the student if the student is at least 23 years old. The Emery School District may expunge medical records and behavioral test assessments. Emery School District will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. Emery School District staff will collaborate with Utah State Archives and Records Services in updating data retention schedules.

Emery School District maintained student-level discipline data will be expunged after three years.

Quality Assurances and Transparency Requirements

Purpose: Data quality is achieved when information is valid for the use to which it is applied, is consistent with other reported data and users of the data have confidence in and rely upon it. Good data quality does not solely exist with the data itself but is also a function of appropriate data interpretation/use and the perceived quality of the data. Thus, true

data quality involves not just those auditing, cleaning and reporting the data, but also data consumers. Data quality is addressed in five areas:

Data Governance Structure

The Emery School District data governance policy is structured to encourage the effective and appropriate use of educational data. The Emery School District data governance structure centers on the idea that data is the responsibility of all Emery School District sections and that data driven decision making is the goal of all data collection, storage, reporting and analysis. Data driven decision making guides what data is collected, reported and analyzed.

Data Requirements and Definitions

Clear and consistent data requirements and definitions are necessary for good data quality. On the data collection side, the Emery School District communicates data requirements and definitions to LEAs through the Data Clearinghouse Update Transactions documentation (see http://www.schools.utah.gov/computerservices/Data-Clearinghouse.aspx). The Emery School District also communicates with LEA IT staff regularly, at monthly Data Warehouse Group meetings and at biannual Data Conferences. Where possible, Emery School District program specialists are invited to these meetings and the same guidance is given to the appropriate LEA program directors.
On the data reporting side, the production and presentation layers provide standard data definitions and business rules. Data Stewards coordinate data releases through the Data Stewards Group meetings. All data released includes relevant data definitions, business rules, and are date stamped. Further, Data and Statistics produces documentation, trainings and FAQs on key statistics and reports, such as proficiency, growth, graduation rate and class size.

Data Collection

Data elements should be collected only once—no duplicate data collections are permitted. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data.
For all new data collections, Emery School District provides to LEAs clear guidelines for data collection and the purpose of the data request. The Emery School District also notifies LEAs as soon as possible about future data collections. Time must be given to LEAs in order for them to begin gathering the data needed.

Data Auditing

Data and Statistics Data Analysts perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with IT and/or LEAs in explaining and/or correcting the anomalies. Data Analysts also work with School Finance to address findings from the Auditors.

Quality Control Checklist

Checklists have been proven to increase quality (See Appendix C). Therefore, before releasing high-risk data, Data Stewards and Data Analysts must successfully complete the data release checklist in three areas: reliability, validity and presentation.

Data Transparency

Annually, Emery School District will publicly post:

- Emery School District data collections
- Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-301

Appendix A: Emery School District Employee Data Privacy Non-Disclosure Agreement

As an employee of the Emery School District, I hereby affirm that:

- I have read the Employee Data Privacy Non-Disclosure Assurances attached to this agreement form and read and reviewed Data Governance Plan Emery School District policies. These assurances address general procedures, data use/sharing, and data security.
- I will abide by the terms of the Emery School District's policies and its subordinate process and procedures;
- I grant permission for the manual and electronic collection and retention of security related information, including but not limited to photographic or video images, of your attempts to access the facility and/or workstations.
- I have read the Emery School District Social Media Policy;
- I have read the Emery School District Communication Policy;
- I have read the Emery School District Bring your own device Policy;

Trainings

- I have completed Emery School District's Data Security and Privacy Fundamentals Training.
- I will complete Emery School District's Data Security and Privacy Fundamentals Training within 30 days of new hire.

Using Emery School District Data and Reporting Systems

- I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.
- I will not share or exchange individual passwords, for either personal computer(s) or Emery School District system user accounts, with Emery School District staff or participating program staff.
- I will log out of and close the browser after each use of Emery School District data and reporting systems.
- I will only access data in which I have received explicit written permissions from the data owner.
- I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, or to publicly release confidential data;

Handling Sensitive Data

- I will keep sensitive data on password-protected state-authorized computers.
- I will keep any printed files containing personally identifiable information in a locked location while unattended.
- I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.
- I will delete files containing sensitive data after working with them from my desktop, or move them to a secured Emery School District server.

Reporting & Data Sharing

- I will not redisclose or share any confidential data analysis except to other authorized personnel without [Emery School District]'s expressed written consent.
- I will not publicly publish any data without the approval of the Superintendent.

- I will take steps to avoid disclosure of personally identifiable information in state-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
- I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.
- I will not transmit child/staff-level data externally unless explicitly authorized in writing.
- I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or within secured server folders is appropriate for Emery School District internal file transfer.
- I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the Emery School District Information Security Officer. Moreover, I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care to prevent disclosure.

Consequences for Non-Compliance

- I understand that access to the Emery School District network and systems can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information;
- I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

Termination of Employment

- I agree that upon the cessation of my employment from Emery School District, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of Emery School District without the prior written permission of the Student Data Manager of Emery School District.

Print Name: _____

Signed: _____

Date: _____

Appendix B: Protecting PII in Public Reporting

Data Gateway Statistical Reporting Method for Protecting PII

Public education reports offer the challenge of meeting transparency requirements while also meeting legal requirements to protect each student's personally identifiable information (PII). Recognizing this, the reporting requirements state that subgroup disaggregation of the data may not be published if the results would yield personally identifiable information about an individual student. While the data used by the Emery School District and local education agencies (LEAs) is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school, LEA, or state-level reports.

This is done by applying the following statistical method for protecting PII.

- Underlying counts for groups or subgroups totals are not reported.
- If a reporting group has 1 or more subgroup(s) with 10 or fewer students.
    - The results of the subgroup(s) with 10 or fewer students are recoded as "N<10"
    - For remaining subgroups within the reporting group

For subgroups with 300 or more students, apply the following suppression rules.

- Values of 99% to 100% are recoded to ≥99%
- Values of 0% to 1% are recoded to ≤1%

For subgroups with 100 or more than but less than 300 students, apply the following suppression rules.

- Values of 98% to 100% are recoded to ≥98%
- Values of 0% to 2% are recoded to ≤2%

For subgroups with 40 or more but less than 100 students, apply the following suppression rules.

- Values of 95% to 100% are recoded to ≥95%
- Values of 0% to 5% are recoded to ≤5%

For subgroups with 20 or more but less than 40 students, apply the following suppression rules.

- Values of 90% to 100% are recoded to ≥90%
- Values of 0% to 10% are recoded to ≤10%
- Recode the percentage in all remaining categories in all groups into intervals as follows (11-19,20-29,…,80-89)

For subgroups with 10 or more but less than 20 students, apply the following suppression rules.

- Values of 80% to 100% are recoded to ≥80%
- Values of 0% to 20% are recoded to ≤20%
- Recode the percentage in all remaining categories in all groups into intervals as follows (20-29,30-39,…,70-79)

Appendix C: Quality Control Checklist

Reliability

- Same definitions were used for same or similar data previously reported or it is made very clear in answering the request how and why different definitions were used
- Results are consistent with other reported results or conflicting results are identified and an explanation provided in request as to why is different
- All data used to answer this request was consistently defined (i.e. if teacher data and student data are reported together, are from the same year/time period)
- Another Emery School District data steward could reproduce the results using the information provided in the metadata

Validity

- Request was clarified
- Identified and included all data owners that would have a stake in the data used
- Data owners approve of data definitions and business rules used in the request
- All pertinent business rules were applied
- Data answers the intent of the request (intent ascertained from clarifying request)
- Data answers the purpose of the request (audience, use, etc.)
- Limits of the data are clearly stated
- Definitions of terms and business rules are outlined so that a typical person can understand what the data represents

Presentation

- Is date-stamped
- Small n-sizes and other privacy issues are appropriately handled
- Wording, spelling and grammar are correct
- Data presentation is well organized and meets the needs of the requester
- Data is provided in a format appropriate to the request
- A typical person could not easily misinterpret the presentation of the data

Technology Security Policy

Purpose: The purpose of this policy is to ensure the secure use and handling of all district data, computer systems and computer equipment by District students, patrons, and employees.

Technology Security: It is the policy of the Emery School District to support secure network systems in the district, including security for all personally identifiable information that is stored on paper or stored digitally on district-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the district, its students, or its employees.

The district will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.

All persons who are granted access to the district network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of district devices and the network. When an employee or other user becomes aware of suspicious activity, he/she is to immediately contact the district's Information Security Officer with the relevant information.

This policy and procedure also covers third party vendors/contractors that contain or have access to Emery School District critically sensitive data. All third party entities will be required to sign the Restriction on Use of Confidential Information Agreement before accessing our systems or receiving information.

It is the policy of Emery School District to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and Privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §63G-2 (hereinafter "GRAMA"), U.C.A. §53E-9-301 et seq and Utah Administrative Code R277-487.

Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network and the Utah State Office of Education. Emery School District supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect Emery School District's data, users, and electronic assets.

Definitions

- Access: Directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.
- Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.
- Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.
- Computer system: A set of related, connected or unconnected, devices, software, or other related computer equipment.
- Computer network: The interconnection of communication or telecommunication lines between computers, or computers and remote terminals, or the interconnection by wireless technology between computers, or computers and remote terminals.

- Computer property: Includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.
- Confidential: Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.
- Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
- Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data, can be considered protected data
- Security system: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.
- Sensitive data - Data that contains personally identifiable information.
- System level – Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

Security Responsibility

- Emery School District shall appoint, in writing, an IT Security Officer (ISO) responsible for overseeing District-wide IT security, to include development of District policies and adherence to the standards defined in this document.

Training

- Emery School District, led by the ISO, shall ensure that all District employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information. Training resources will be provided to all District employees.
- Emery School District, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.

Physical Security

- Computer Security
    - Emery School District shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. Automatic log off, locks and password screen savers should be used to enforce this requirement.
    - Emery School District shall ensure that all equipment that contains sensitive information will be secured to deter theft.
- Server/Network Room Security
    - Emery School District shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or District office areas. Access control shall be enforced using either keys, electronic card readers, or similar method with only those IT or other staff members having access necessary to perform their job functions are allowed unescorted access.
    - Telecommunication rooms/closets may only remain unlocked or unsecured when because of building design it is impossible to do otherwise or due to environmental problems that require the door to be opened.
- Contractor access

- Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor will need to present a company issued identification card, and his/her access will need to be confirmed directly by the authorized employee who issued the service request or by Emery School District's Technology Department.

Network Security

- Network perimeter controls will be implemented to regulate traffic moving between trusted internal (District) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.
- Network Segmentation
  - Emery School District shall ensure that all untrusted and public access computer networks are separated from main district computer networks and utilize security policies to ensure the integrity of those computer networks.
  - Emery School District will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.
- Wireless Networks
  - No wireless access point shall be installed on Emery School District's computer network that does not conform with current network standards as defined by the Network Manager. Any exceptions to this must be approved directly in writing by the Information Security Officer.
  - Emery School District shall scan for and remove or disable any rogue wireless devices on a regular basis.
  - All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.
- Remote Access
  - Emery School District shall ensure that any remote access with connectivity to the District's internal network is achieved using the District's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the Information Security Officer.

Access Control

- System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.
- Authentication
  - Emery School District shall enforce strong password management for employees, students, and contractors.
  - Password Creation
    - All server system-level passwords must conform to the Password Construction Guidelines posted on the Emery School District Technology Website.
- Password Protection
  - Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
  - Passwords must not be inserted into email messages or other forms of electronic communication.
  - Passwords must not be revealed over the phone to anyone.
  - Do not reveal a password on questionnaires or security forms.

    - Do not hint at the format of a password (for example, "my family name").
    - Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
- Authorization
    - Emery School District shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.
    - Emery School District shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.
- Accounting
    - Emery School District shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.
- Administrative Access Controls
    - Emery School District shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

Incident Management

- Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

Business Continuity

- To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of District IT operations.
- Emery School District shall develop and deploy a district-wide business continuity plan which should include as a minimum:
    - Backup Data: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.
    - Secondary Locations: Identify a backup processing location, such as another School or District building.
    - Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuing a full head count of all.

Malicious Software

- Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.
- Emery School District shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.
- Emery School District shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.
- Emery School District shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.

- All computers must use the District approved anti-virus solution.
- Any exceptions to section 3.9 must be approved by the Information Security Officer.

Internet Content Filtering

- In accordance with Federal and State Law, Emery School District shall filter internet traffic for content defined in law that is deemed harmful to minors.
- Emery School District acknowledges that technology based filters are not always effective at eliminating harmful content and due to this, Emery School District uses a combination of technological means and supervisory means to protect students from harmful online content.
- In the event that students take devices home, Emery School District will provide a technology based filtering solution for those devices. However, the District will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content.
- Students shall be supervised when accessing the internet and using district owned devices on school property.

Data Privacy

- Emery School District considers the protection of the data it collects on students, employees and their families to be of the utmost importance.
- Emery School District protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 ("FERPA"), the Government Records and Management Act U.C.A. §63G-2 ("GRAMA"), U.C.A. §53E-9-301 et seq, 15 U.S. Code §§ 6501–6506 ("COPPA") and Utah Administrative Code R277-487 ("Student Data Protection Act").
- Emery School District shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

Security Audit and Remediation

- Emery School District shall perform routine security and privacy audits in congruence with the District's Information Security Audit Plan.
- District personnel shall develop remediation plans to address identified lapses that conforms with the District's Information Security Remediation Plan Template.

Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and District policies. Any employee found to be in violation may be subject to disciplinary action up to and including termination of employment with the Emery School District.

Family Educational Rights and Privacy Act (FERPA) Notice for Directory Information

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that Emery School District, with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, Emery School District may disclose appropriately designated "directory information" without written consent, unless you have advised the District to the contrary in accordance with District procedures. The primary purpose of directory information is to allow the Emery School District to include this type of information from your child's education records in certain school publications. Examples include:

- A playbill, showing your student's role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs; and
- Sports activity sheets, such as for wrestling, showing weight and height of team members.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks. In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA) to provide military recruiters, upon request, with the following information – names, addresses and telephone listings – unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent.

If you do not want Emery School District to disclose directory information from your child's education records without your prior written consent, you must notify the District in writing. Emery School District has designated the following information as directory information:

- Student's name
- Participation in officially recognized activities and sports
- Address
- Weight and height of members of athletic teams
- Telephone listing
- Degrees, honors, and awards received
- Electronic mail address
- Date and place of birth
- Photograph
- The most recent educational agency or institution attended
- Major field of study
- Dates of attendance
- Grade level
- Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems that cannot be used to access education records without a PIN, password, etc. (A student's SSN, in whole or in part, cannot be used for this purpose.)

DATA OWNERSHIP & ACCESS GUIDELINES

- Emery School District will require a signed and dated written request, which must include the person's name, address, phone number, student's name, student identification number (SIN), school name in which their student is enrolled, relationship to the student, items requested for review, and reason for making the request.
- Emery School District will require proof of identity and relationship to the student before access to records is granted.
- Requests for access to any Emery School District secure materials will require a signed security/confidentiality agreement prior to inspection.
- Any proper request for access to inspect and review any personally identifiable data by the eligible student or the student's parents will be granted without unnecessary delay and no more than 45 days after the request is made and the right to access is established by proof of identity and a signed security/confidentiality agreement, if requesting secure materials.
- If any record includes data on more than one child, the parents shall be allowed to inspect and review only those records relevant to their child.
- Parents shall be provided a response to reasonable requests for explanation or interpretation of the data.
- Parents and students, when applicable, have the right to a due process hearing to challenge the content of their child's record or to ensure that the records are accurate and in no way violate the student's right to privacy.

Emery School District Prohibited Activities without Prior Consent

In accordance with 53E-9-202 and 53E-9-203, LEAs shall adopt policies governing the protection of family and student privacy. These policies shall require prior written consent of the parent or legal guardian of a student before administering and collecting the information listed below, whether information is personally identifiable or not.

Prohibited Activities:
Any psychological or psychiatric examination, test, or treatment, or any survey, analysis, or evaluation, in which the purpose or intended effect is to cause the student to reveal information concerning the student's or any family member's:

- political affiliations or political philosophies
- mental or psychological problems
- sexual behavior, orientation, or attitudes
- illegal, anti-social, self-incriminating, or demeaning behavior
- critical appraisals of individuals with whom the student or family member
- has close family relationships
- religious affiliations or beliefs
- legally recognized privileged and analogous relationships, such as those with
- lawyers, medical personnel, or ministers and
- income, except as required by law.

A general consent used to approve admission to school or involvement in special education, remedial education, or a school activity does not constitute written consent under this policy. Prior written consent shall be required from the parent or legal guardian of a student in all grades, kindergarten through grade 12. Prior written consent shall be required for activities within the curriculum as well as other activities.

Requirements for Valid Prior, Written Consent:
Parent shall be provided written notice, at least two weeks prior to administration (except in response to a situation which a school employee reasonably believes to be an emergency, or as authorized under Title 62A, Chapter 4a, Part 4, Child Abuse or Neglect Reporting Requirements, or by order of a court). Following disclosure, a parent or guardian may waive the two-week minimum notification period.

This notice shall include:

- Notice that a copy of the educational or student survey questions is made available at the school
- An Internet address where a parent or legal guardian can view the exact survey to be administered
- Reasonable opportunity to obtain written information concerning:
    - records or information, including information about relationships, that may be examined or requested
    - how the records or information shall be examined or reviewed
    - how the information is to be obtained
    - the purposes for which the records or information are needed
    - the entities or persons, regardless of affiliation, who will have access
    - to the personally identifiable information and
    - a method by which a parent of a student can grant permission to access or examine the personally identifiable information.

Authorization: The prior consent is valid only for the activity for which it was granted, unless otherwise agreed to by a student's parent or legal guardian and the person requesting written consent. To terminate the authorization, the authorizing parent or guardian shall submit a written withdrawal of authorization to the school principal.

Exceptions: If a school employee or agent believes that a situation exists which presents a serious threat to the well-being of a student, that employee or agent shall notify the student's parent or guardian without delay, unless the matter has been reported to the Division of Child and Family Services within the Department of Human Services.

If a school employee, agent, or school resource officer believes a student is at-risk of attempting suicide, physical self-harm, or harming others, the school employee, agent, or school resource officer may intervene and ask a student questions regarding the student's suicidal thoughts, physically self-harming behavior, or thoughts of harming others for the purposes of:

- referring the student to appropriate prevention services; and
- informing the student's parent or legal guardian.

In accordance with §53G-9-604, schools shall notify parents or legal guardians of such threats and incidents. Following parent notification of student suicide threat, bullying incident, cyber-bullying incident, harassment incident, hazing incident or retaliation incident, schools shall maintain a record of the notification, securely and confidentially, consistent with §53G-9-604.

A sample record of parental notification is provided.

RECORD OF PARENT NOTIFICATION OF STUDENT THREAT OR INCIDENT FORM
Required by 53G-9-604

This form is a record required to be maintained securely and confidentially by the school consistent with §53G-9-604 following parent notification of student suicide threat, bullying incident, cyber-bullying incident, harassment incident, hazing incident or retaliation incident. THIS FORM SHOULD NOT BE USED TO NOTIFY PARENT(S) OF THE INCIDENT.

Student's name: _____

Parent(s) name: _____

Date of incident: _____

Parent was notified of the incident by:

_____ _____
Designated School Employee's Name Signature

on_____by phone___email___

mail___other___ Date_____

Provide parent contact information:

_____

_____

Parent was notified of:___ suicide threat

___ bullying incident
___cyber-bullying incident
___ harassment incident
___ hazing incident
___retaliation incident

Utah LEAs and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53E-9-301, and comply with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with 53E-9-301, the LEAs shall expunge student data that is stored by the education entity upon request of the student if the student is at least 23 years old. The LEAs may expunge medical records and behavioral test assessments. An education entity shall not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information.

An LEA or school may create and maintain a cumulative disciplinary record for a student.

Emery School District Employee Data Sharing and Confidentiality Agreement

To minimize the risk of human error and misuse of information, Emery School District will provide a range of training opportunities for all Emery School District staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records.

All Emery School District employees and contracted partners must sign and obey the Emery School District Employee Acceptable Use Policy, which describes the permissible uses of state technology and information. Emery School District employees and contracted partners also must sign and obey the Emery School District Employee Data Sharing and Confidentiality Agreement, which describes appropriate uses and the safeguarding of student and educator data. New Emery School District employees must sign the aforementioned documents prior to being granted access to Emery School District systems.

As of the adoption of this policy, existing Emery School District employees will be given 90 days to complete the required training and sign the aforementioned documents. Thereafter, all employees will be required to participate in an annual Data Security and Privacy Fundamentals training, which is mandatory for continued access to the Emery School District network. These signed agreements will be maintained in the employee's file in Emery School District human resources office. Non-compliance with the agreements shall result in consequences up to and including removal of access to the Emery School District network; if this access is required for employment, employees and contractors may be subject to dismissal.

Additionally, Emery School District requires targeted information security and privacy training for specific groups within the agency and provides updated guidance to local education agencies concerning compliance with state and federal privacy laws and best practices in this ever-changing environment.

Emery School District Data Sharing Agreement

Prior to sharing personally identifiable student information for purposes of educational studies on behalf of educational agencies or institutions, Emery School District must enter into a written agreement. This agreement establishes the terms and conditions under which the Emery School District will grant access of personally identifiable information (PII) from education records to _____. Requirements for data sharing agreements to disclose student data for studies on behalf of educational agencies or institutions:

Study Description: purpose of the study to be conducted; scope of the proposed study; duration of the study, and information to be disclosed.

Emery School District will not disclose all of the personally identifiable information from its education records; it will determine only the specific elements the authorized representative needs and disclose only those. Agreement requires the authorized representative to use personally identifiable information only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure. Approval to use the personally identifiable information (PII) from the education records for one study, audit, or evaluation does not confer approval to use it for another.

This agreement requires the authorized representative to conduct the study in a manner that does not permit the personal identification of parents and students by anyone other than representatives of the organization with legitimate interests. The agreement requires the authorized representative to conduct the study not identifying students or their parents. The authorized representative will allow internal access to personally identifiable information (PII) from education records only to individuals with a need to know for the purposes of the study. The authorized representative will take steps to maintain the confidentiality of the personally identifiable information (PII) at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques.

Monitoring implementation of data sharing agreements:

In addition to all of the precautions addressed above, agreement requires the following assurances to protect personally identifiable (PII) information from further disclosure and unauthorized use:

- Emery School District may require the authorized representative to provide a certification indicating that an independent vulnerability or risk assessment of this data security program has occurred. Emery School District maintains the right to inspect the authorized representative's premises or technology used to transmit or maintain data
- Emery School District may request the organization's policies and procedures to protect privacy and data security, including the ongoing management of data collection, processing, storage, maintenance, use, and destruction. Emery School District may also verify that the authorized representative has a training program to teach its employees about FERPA, and to protect personally identifiable information from education records
- If applicable, Emery School District may verify that the authorized representative has appropriate disciplinary policies for employees that violate FERPA, including termination in appropriate instances
- Emery School District maintains the right to conduct audits or other monitoring activities of the authorized representative's data stewardship policies, procedures, and systems. If, through these monitoring activities, a vulnerability is found, the authorized representative must take timely appropriate action to correct or mitigate any weaknesses discovered; and
- Emery School District maintains the right to review any data prior to publication and to verify that proper disclosure avoidance techniques are used, and maintains the right to approve reports prior to publication to ensure they reflect the original intent of the agreement

Consequences for failure to comply with data sharing agreements

An individual may file a written complaint with Emery School District regarding an alleged violation of a data sharing agreement or contract. A complaint must contain specific allegations of fact giving reasonable cause to believe that a violation of a data sharing agreement or contract has occurred. Emery School District will investigate all reasonable and timely complaints. Emery School District may also conduct its own investigation without a complaint, or if a complaint has been withdrawn, to determine whether a violation has occurred.

As required by FERPA, if an authorized representative that receives data to perform evaluations, audits, or compliance activities improperly discloses the data, Emery School District shall deny that representative further access to personally identifiable data for at least five years. In addition, Emery School District may pursue penalties permitted under state contract law, such as liquidated damages.

By the signatures of representatives below, Emery School District and _____, intending to be legally bound, agree to all of the provisions of this Data Sharing Agreement.

Name of representative of Applying Entity/Organization_____

Signature: _____Date: _____

Emery School District representative _____

Signature: _____Date: _____

Emery School District Data Sharing Agreement
(Audits, Evaluation or Compliance Monitoring)

Prior to sharing personally identifiable student information for purposes of educational studies for audits, evaluation or compliance monitoring, Emery School District must enter into a written agreement. This agreement establishes the terms and conditions under which the Emery School District will grant access to personally identifiable information (PII) from education records to _____ (Applying Entity/Organization)

Requirements for data sharing agreements to disclose student data for audits, evaluation or compliance monitoring

Study Description:

- purpose of the study to be conducted
- scope of the proposed study
- duration of the study, and
- information to be disclosed
- State specifically that the disclosure is for an audit, evaluation, or enforcement or compliance activity. This agreement must specify the student information being disclosed and must include a description of how the student data will be used. This agreement must describe methodology and why disclosure of personally identifiable student information is necessary to carry out the audit, evaluation, or enforcement or compliance activity.

Designated individual or entity that will serve as the authorized representative:

_____

*If an entity, specify the individuals directly responsible for managing the requested data

Authorized representative will use personally identifiable information only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure.

Authorized representative must destroy the personally identifiable information (PII) from the education records when the information is no longer required for the purpose specified and must be clear about how the education records were destroyed. The agreement must identify a specific time for destruction based on the facts and circumstances surrounding the disclosure and study. Emery School District may extend the time if needed.

The agreement requires the authorized representative to provide written confirmation to Emery School District when education records are destroyed;

- Documents appropriate technical, physical, and administrative safeguards to protect personally identifiable student data at rest and in transit.

- This agreement requires procedures to protect personally identifiable student information from further disclosure and unauthorized use, including limiting use of personally identifiable information(PII) to only the authorized representatives with a legitimate interests in the audit, evaluation, or enforcement or compliance activity; and

- Include a plan for responding to a breach in security, and report any breach immediately to Emery School District.

Emery School District will not disclose all of the personally identifiable information (PII) from its education records; it will determine only the specific elements the authorized representative needs and disclose only those. Agreement

requires the authorized representative to use personally identifiable information (PII) only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure. Approval to use the personally identifiable information (PII) from the education records for one study, audit, or evaluation does not confer approval to use it for another.

Monitoring implementation of data sharing agreements:

In addition to all of the precautions addressed above, agreement requires the following assurances to protect personally identifiable information (PII) from further disclosure and unauthorized use:

- Emery School District may require the authorized representative to provide a certification indicating that an independent vulnerability or risk assessment of this data security program has occurred. Emery School District shall also maintain the right to inspect the authorized representative's premises or technology used to transmit or maintain data
- Emery School District may also verify that the authorized representative has a training program to teach its employees about FERPA, and to protect personally identifiable information from education records
- If applicable, Emery School District may verify that the authorized representative has appropriate disciplinary policies for employees that violate FERPA, including termination in appropriate instances
- Emery School District maintains the right to conduct audits or other monitoring activities of the authorized representative's data stewardship policies, procedures, and systems. If, through these monitoring activities, a vulnerability is found, the authorized representative must take timely appropriate action to correct or mitigate any weaknesses discovered; and
- Emery School District maintains the right to review any data prior to publication and to verify that proper disclosure avoidance techniques are used, and maintains the right to approve reports prior to publication to ensure they reflect the original intent of the agreement

Consequences for failure to comply with data sharing agreements

An individual may file a written complaint with Emery School District regarding an alleged violation of a data sharing agreement or contract. A complaint must contain specific allegations of fact giving reasonable cause to believe that a violation of a data sharing agreement or contract has occurred. Emery School District will investigate all reasonable and timely complaints. Emery School District may also conduct its own investigation without a complaint, or if a complaint has been withdrawn, to determine whether a violation has occurred.

As required by FERPA, if an authorized representative that receives data to perform evaluations, audits, or compliance activities improperly discloses the data, Emery School District shall deny that representative further access to personally identifiable data for at least five years. In addition, Emery School District may pursue penalties permitted under state contract law, such as liquidated damages.

By the signatures of representatives below, Emery School District and _____, intending to be legally bound, agree to all of the provisions of this Data Sharing Agreement.

Name of representative of Applying Entity/Organization_____

Signature: _____Date: _____

Emery School District representative _____

Signature: _____Date: _____

Emery School District
Employee Data Privacy Non-Disclosure Agreement

As an employee of the Emery School District, I hereby affirm that: (Initial)

- I have read the Employee Non-Disclosure Assurances attached to this agreement form and have read and reviewed Data Governance Plan and Emery School District policies. These assurances address general procedures, data use/sharing, and data security
- I will abide by the terms of the Emery School District's policies and its subordinate process and procedures
- I grant permission for the manual and electronic collection and retention of security-related information, including but not limited to, photographic or video images and attempts to access the facility and/or workstations
- I have read the Emery School District Social Media Policy
- I have read the Emery School District Communication Policy
- I have read the Emery School District Bring your own device Policy

Trainings

- I have completed Emery School District's Data Security and Privacy Fundamentals Training.
- I will complete Emery School District's Data Security and Privacy Fundamentals Training within 30 days of new hire

Using Emery School District Data and Reporting Systems

- I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.
- I will not share or exchange individual passwords, for either personal computer(s) or Emery School District system user accounts, with Emery School District staff or participating program staff.
- I will log out of and close the browser after each use of Emery School District data and reporting systems.
- I will only access data in which I have received explicit written permission from the data owner.
- I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, or to publicly release confidential data

Handling Sensitive Data

- I will keep sensitive data on password-protected state-authorized computers.
- I will keep any printed files containing personally identifiable information in a locked location while unattended.
- I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.
- I will delete files containing sensitive data after working with them from my desktop, or move them to a secured Emery School District server.
- Reporting & Data Sharing
- I will not re-disclose or share any confidential data analysis except to other authorized personnel without Emery School District's expressed written consent.
- I will not publicly publish any data without the approval of the Superintendent.

- I will take steps to avoid disclosure of personally identifiable information in state-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
- I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.
- I will not transmit child/staff-level data externally unless explicitly authorized in writing.
- I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or within secured server folders appropriate for Emery School District internal file transfer.
- I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the Emery School District Information Security Officer. Moreover, I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care to prevent disclosure.

Consequences for Non-Compliance

- I understand that access to the Emery School District network and systems can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information
- I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

Termination of Employment

- I agree that upon the cessation of my employment from Emery School District, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of Emery School District without the prior written permission of the Student Data Manager of Emery School District.

Print Name: _____

Signed: _____

Date: _____