MURRAY CITY SCHOOL DISTRICT

NUMBER:	ADM 230
EFFECTIVE:	3/12/2000
REVISION:	
PAGES:	15

Statement of.....

Policy and Responsibility

SUBJECT: DATA PRIVACY, SECURITY, and GOVERNANCE POLICY

Data Privacy and Security

The efficient collection, analysis, and storage of student and employee information is essential to improve the education of our students and the smooth operation of the district. As the use of data has increased and technology has advanced, the need to exercise care in the handling of confidential information has intensified. The privacy of students and employees and the use of confidential information is protected by federal and state laws, including the Family Educational Rights and Privacy Act (FERPA).

Defined Terms

Administrative Security consists of policies, procedures, and personnel controls including security policies, training, and audits, technical training, supervision, separation of duties, rotation of duties, recruiting and termination procedures, user access control, background checks, performance evaluations, and disaster recovery, contingency, and emergency plans. These measures ensure that authorized users know and understand how to properly use the system in order to maintain security of data.

Aggregate Data is collected or reported at a group, cohort or institutional level and does not contain personally identifiable information (PII).

Data Breach is the unauthorized acquisition of PII.

Employee Data means data collected and included in an employee's employment records.

Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights and authority levels. These measures ensure that only authorized users are able to perform actions or access information in a network or a workstation.

Personally Identifiable Information (PII) includes: a student/employee's name; the name

of a student/employee's family; the a student/employee's address; the a student/employee's social security number; a student/employee's unique identification number or biometric record; or other indirect identifiers such as a date of birth, place of birth or mother's maiden name; and other information that alone or in combination is linked or linkable to a specific student/employee that would allow a reasonable person in the school community who does not have personal knowledge of the relevant circumstances, to identify the student.

Physical Security describes security measures designed to deny unauthorized access to facilities or equipment.

Student Data means data collected at the student level and included in a student's educational records.

Unauthorized Data Disclosure is the intentional or unintentional release of PII to an unauthorized person or untrusted environment.

Collection

- The district shall follow applicable state and federal laws related to student/employee privacy in the collection of data.

Access

- Unless prohibited by law or court order, the district shall provide parents, legal guardians, or eligible students, as applicable, the ability to review their child's educational records.

- The Superintendent, administrator, or designee, is responsible for granting, removing, and reviewing user access to student/employee data. An annual review of existing access shall be performed.

- Access to PII maintained by the district shall be restricted to: (1) the authorized staff of the school district or public charter school who require access to perform their assigned duties; and (2) authorized employees of the State Board of Education and the State Department of Education who require access to perform their assigned duties; and (3) vendors who require access to perform their contracted/assigned duties.

Security

- The district shall have in place Administrative Security, Physical Security, and Logical Security controls to protect from a Data Breach or Unauthorized Data Disclosure.

- The district shall notify in a timely manner affected individuals, students, employees, and families if there is a confirmed Data Breach or confirmed Unauthorized Data Disclosure.

Use

Publicly released reports shall not include PII and shall use Aggregate Data in such a manner that re-identification of individual students or employees is not possible.

- If the district contracts with outside vendors involving student data, which govern databases, online services, assessments, special education or instructional supports, shall include the following provisions which are intended to safeguard student privacy and the security of the data:
    - Requirement that the vendor agree to comply with all applicable state and federal law;
    - Requirement that the vendor have in place Administrative Security, Physical Security, and Logical Security controls to protect from a Data Breach or Unauthorized Data Disclosure;
    - Requirement that the vendor restrict access to PII to the authorized staff of the vendor who require such access to perform their assigned duties;
    - Prohibition against the vendor's secondary use of PII including sales, marketing or advertising;
    - Requirement for data destruction and an associated timeframe; and
    - Penalties for non-compliance with the above provisions.
- The district shall clearly define what data is determined to be directory information.
- If the district chooses to publish student directory information which includes PII, parents must be notified annually in writing and given an opportunity to opt out of the directory. If a parent does not opt out, the release of the information as part of the directory is not a Data Breach or Unauthorized Data Disclosure.

Data Governance

PURPOSE

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 Murray City School District takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401 requires that Murray City School District adopt a Data Governance Plan.

SCOPE AND APPLICABILITY

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

1. Data Advisory Groups
2. Non-Disclosure Assurances for Employees
3. Data Security and Privacy Training for Employees
4. Data Disclosure
5. Data Breach
6. Record Retention and Expungement
7. Data Quality
8. Transparency

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

1. Designates Murray City School District as the steward for all confidential information maintained within Murray City School District.
2. Designates Data Stewards access for all confidential information.
3. Requires Data Stewards to maintain a record of all confidential information that they are responsible for.
4. Requires Data Stewards to manage confidential information according to this plan and all other applicable policies, standards and plans.
5. Complies with all legal, regulatory, and contractual obligations regarding privacy of Agency data. Where such requirements exceed the specific stipulation of this plan, the legal, regulatory, or contractual obligation shall take precedence.
6. Provides the authority to design, implement, and maintain privacy procedures Murray City School District standards concerning the privacy of data in motion, at rest and processed by related information systems.
7. Ensures that all Murray City School District board members, employees, contractors, and volunteers comply with the policy and undergo annual privacy training.
8. 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 GROUP

Structure

Murray City School District has a district leadership team, which consists of school and district leadership who have responsibility for providing data to internal and external stakeholders as appointed by the Superintendent.

Individual and Group Responsibilities

The following tables outline individual Murray City School District staff and advisory group responsibilities.

Table 1. Individual Murray City School District Staff Responsibilities

Role	Responsibilities
LEA Student Data Manager (District Technology Coordinator)	1. May authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity 2. Acts as the primary local point of contact for the state student data officer. 3. May share personally identifiable student data that is: a. about a student with the student and the student's parent b. required by state or federal law c. in an aggregate form with appropriate data redaction techniques applied d. for a school official e. for an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court f. in response to a subpoena issued by a court. g. directory information h. in response to submitted data requests from external researchers or evaluators, 4. May not share personally identifiable student data for the purpose of external research or evaluation. 5. Will create and maintain a list of all LEA staff that have access to personally identifiable student data. 6. Ensure all members, including volunteers, receive annual LEA level training on data privacy. Document all staff names, roles, and training dates, times, locations, and agendas.
IT Systems Security Manager (District Technology Coordinator)	1. Acts as the primary point of contact for state student data security ; 2. Ensures compliance with security systems laws throughout the public education system, including: a. providing training and support to applicable Murray City School District employees; and b. producing resource materials, model plans, and model forms for District systems security; 3. Investigates complaints of alleged violations of systems breaches; 4. Provides an annual report to the board on the District's systems security needs.
Teaching & Learning Team Directors	1. Acts at the primary point of contact for external research requests. 2. Directs staff who provide reports to internal stakeholders.

EMPLOYEE NON-DISCLOSURE ASSURANCES

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

Scope

All Murray City School District board members, employees, contractors and volunteers must sign and obey the Murray City 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 Murray City 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 Murray City School District is protected in accordance with the Family Educational Rights and Privacy Act (FERPA) and Utah law. This plan outlines the way District staff are to utilize data and protect personally identifiable and confidential information. An electronically signed agreement form is required from all District staff to verify agreement to adhere to/abide by these practices and will be maintained with the District's Human Resources Director. All Murray City School District employees (including contract or temporary) will:

1. Complete a Security and Privacy Fundamentals Training.
2. Complete a Security and Privacy Training for Researchers and Evaluators, if your position is a research analyst or if requested by the Superintendent.
3. Consult with Murray City School District internal data owners when creating or disseminating reports containing data.
4. Use password-protected state-authorized computers when accessing any student-level or staff-level records.
5. NOT share individual passwords for personal computers or data systems with anyone.
6. Log out of any data system/portal and close the browser after each use.
7. Store sensitive data on a appropriate-secured location. 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.
8. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at Murray City School District when disposing of such records.
9. 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.
10. Redact 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).
11. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

12. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
13. 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.
14. Use secure methods when sharing or transmitting sensitive data. The approved method is Murray City School District's Secure File Transfer Protocol (SFTP) website. Also, sharing within secured server folders (S Drive) is appropriate for Murray City School District internal file transfer.
15. 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.
16. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

Data security and privacy training

Purpose

Murray City 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

These training requirements are applicable to 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

1. Within the first week of employment, all District board members, employees, and contracted partners must sign and follow the District's Employee Acceptable Use Policy, which describes the permissible uses of state technology and information. All volunteers must sign and follow the District's Employee Acceptable Use Policy prior to volunteering. Within two weeks of the commencements of their term on the Board fo Education, each Board member must review and agree to comply with the District's Employee Acceptable Use Policy.
2. New employees that do not comply may not be able to use Murray City School District networks or technology. Within the first week of employment, all Murray City School District board members, employees, and contracted partners also must review, electronically sign, and follow the District Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current Murray City 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 plan.
4. Murray City School District requires a targeted Security and Privacy Training for Data Stewards and IT staff for other specific groups within the agency that collect, store, or disclose data. The Student Data Manager will identify these groups and will determine the annual training topics for these targeted groups based on Murray City School District training needs.
5. 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

Murray City 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 Murray City School District increases transparency, promotes education in Murray City School District, and increases knowledge about Utah public education. This plan establishes the protocols and procedures for sharing data maintained by the 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 §53A-1-1401.

Policy for disclosure of Personally Identifiable Information (PII)

Student or Student's Parent/Guardian Access

In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), Murray City School District will provide parents with access to their child's education records, or provide an eligible student access to his or her own educational 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. The School/District is not required to provide data that it does not maintain, nor is Murray City 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 Murray City School District must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401. Vendors determined not to be compliant may be prohibited from entering into future contracts with Murray City School District without third-party verification that they are compliant with federal and state law, and board policy.

Internal Partner Requests

Internal partners to Murray City 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 the District's data request ticketing system.

Governmental Agency Requests

Murray City School District may not disclose personally identifiable information of students to a 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

a) reporting requirement
b) audit
c) evaluation

The Student Data Manager 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."

Policy for 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

Murray City 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 Student Data Manager 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 completes a Request to do Research Form and submits it to the Director of Teaching & Learning.

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 completes a Request to do Research Form and submits it to the Director of Teaching & Learning.

High-Risk Data Request Process

Definition: Student-level data that are de-identified.

Examples:

- De-identified student-level graduation data
- De-identified student-level SAGE ELA assessment scores for grades 3-6.

Process: Requester completes a Request to do Research Form and submits it to the Director of Teaching & Learning.

Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The Student Data Manager will ensure the proper data are shared with external researcher or evaluator to comply with federal, state, and board rules.
Murray City 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:

1. A Murray City School District Director, Superintendent, or board member sponsors an external

researcher or evaluator request.
2. Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Student Data Manager.
3. Researchers and evaluators supply the Murray City School District a copy of any publication or presentation that uses Murray City School District data 10 business days prior to any publication or presentation.

Process: Research Proposal must be submitted using the form available from Murray School District. Research proposals are sent directly to the Communication and Public Information Coordinator for review. If the request is approved, the request placed on the board agenda to be presented by a member of the Teaching & Learning Team for approval of the board.

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.

Procedures

Murray City 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, Murray City School District staff shall follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, Murray City 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 Murray City School District administrative team to determine whether a security breach has occurred. If the Murray City School District data breach response team determines that one or more employees or contracted partners have substantially failed to comply with the District's IT Security Plan 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. Murray City School District will provide an periodically update, in keeping with industry best practices, resources for LEA staff, faculty, and volunteers in preparing for and responding to a security breach. Murray City School District will make these resources available in its website.

Record Retention and Expungement

Purpose

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

Scope

This applies to all Murray City School District board members and staff.

Policy

The Murray City School District, staff, and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53A-1-1407, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

The District may expunge medical records and behavioral test assessments. The District will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. Murray City School District staff will collaborate with Utah State Achieves and Records Services in updating data retention schedules.
Murray City School District maintained student-level discipline data will be expunged after three years.
7. Expungement Request Policy
The LEA recognizes the risk associated with data following a student year after year that could be used to mistreat the student. The LEA shall review all requests for records expungement from parents and make a determination based on the following procedure.
7.1 Procedure
The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information. The procedure for expungement shall match the record amendment procedure found in 34 CFR 99, Subpart C of FERPA.

- If a parent believes that a record is misleading, inaccurate, or in violation of the student's privacy, they may request that the record be expunged.
- The LEA shall decide whether to expunge the data within a reasonable time after the request.
- If the LEA decides not to expunge the record, they will inform the parent of their decision as well
- as the right to an appeal hearing.
- The LEA shall hold the hearing within a reasonable time after receiving the request for a hearing.
- The LEA shall provide the parent notice of the date, time, and place in advance of the hearing.
- The hearing shall be conducted by any individual that does not have a direct interest in the
- outcome of the hearing.
- The LEA shall give the parent a full and fair opportunity to present relevant evidence. At the
- parents' expense and choice, they may be represented by an individual of their choice, including
- an attorney.
- The LEA shall make its decision in writing within a reasonable time following the hearing.
- The decision must be based exclusively on evidence presented at the hearing and include a
- summary of the evidence and reasons for the decision.
- If the decision is to expunge the record, the LEA will seal it or make it otherwise unavailable to
- other staff and educators.

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 and 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 at is addressed in five areas:

Data Governance Structure

The Murray City School District data governance policy is structured to encourage the effective and appropriate use of educational data. The District data governance structure centers on the idea that data is the responsibility of all District schools and departments 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 District receives training from and regularly communicates with the Utah State Board of Education and Utah Education Network regarding data requirements and definitions. The Murray City School District also communicates with LEA IT staff regularly at staff meetings, district leadership team

meetings, and mentor meetings. Where possible, 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 in accordance with the Utah Board of Education requirements.

Data Auditing

The District technology department and supporting staff perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with to explain or correct the anomalies. The District Technology Departments also work with the Business Administrator and supporting staff 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, Murray City School District will publically post:

- Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401
- Murray School District Data Collections

Appendix

Appendix A. Murray City School District Employee Non-Disclosure Agreement

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

_____ I have read the Employee Non-Disclosure Assurances attached to this agreement form and read and reviewed Data Governance Plan Murray City School District policies. These assurances address general procedures, data use/sharing, and data security.

_____ I will abide by the terms of the Murray City School District's policies and corresponding district plans, 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 videotape images, of your attempts to access the facility and/or workstations.

Trainings

_____ I have completed Murray City School District's Data Security and Privacy Fundamentals Training.

Or

_____ I will completed Murray City School District's Data Security and Privacy Fundamentals Training within 30 days.

Using Murray City 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 Murray City School District system user accounts, with Murray City School District staff or participating program staff.

_____I will lock or close my computer whenever I leave my computer unattended.

_____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 LEA-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 Murray City School District server (S or U Drive).

Reporting & Data Sharing

_____ I will not disclose, share, or publish any confidential data analysis without the approval of my supervisor.

_____ I will take steps to avoid disclosure of personally identifiable information in LEA or school-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

_____ I will <u>not</u> 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 student/staff-identifying data with authorized individuals, the only approved methods are phone calls or Murray City School District's Secure File Transfer Protocol (SFTP). Also, sharing within secured server folders is appropriate for Murray City School District internal file transfer (S Drive).

_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the Murray City School District Technology Coordinator. 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 Murray City 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 Murray City School District, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of Murray City School District without the prior written permission of the Student Data Manager of Murray City School District.

Print Name: _____

Signed: _____

Date: _____

Appendix B. Protecting PII in Public Reporting

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 Murray City 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-level reports.

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

1. Underlying counts for groups or subgroups totals are not reported.
2. 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
        1. For subgroups with 300 or more students, apply the following suppression rules.
            1. Values of 99% to 100% are recoded to ≥99%
            2. Values of 0% to 1% are recoded to ≤1%
        2. For subgroups with 100 or more than but less than 300 students, apply the following suppression rules.
            1. Values of 98% to 100% are recoded to ≥98%
            2. Values of 0% to 2% are recoded to ≤2%
        3. For subgroups with 40 or more but less than 100 students, apply the following suppression rules.
            1. Values of 95% to 100% are recoded to ≥95%
            2. Values of 0% to 5% are recoded to ≤5%
        4. For subgroups with 20 or more but less than 40 students, apply the following suppression rules.
            1. Values of 90% to 100% are recoded to ≥90%
            2. Values of 0% to 10% are recoded to ≤10%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (11-19,20-29,…,80-89)
        5. For subgroups with 10 or more but less than 20 students, apply the following suppression rules.
            1. Values of 80% to 100% are recoded to ≥80%
            2. Values of 0% to 20% are recoded to ≤20%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (20-29,30-39,…,70-79)

Appendix C. Example Quality Control Checklist

Reliability (results are consistent)

1. 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
2. Results are consistent with other reported results **or** conflicting results are identified and an explanation provided in request as to why is different
3. All data used to answer this particular request was consistently defined (i.e. if teacher data and student data are reported together, are from the same year/time period)
4. Another Murray City School District data steward could reproduce the results using the information provided in the metadata

Validity (results measure what are supposed to measure, data addresses the request)

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

Presentation

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