**7100 Data Governance Plan**

Approved: 10 December 2019

1. Purpose
    a. 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. Maeser 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 Maeser adopt a Data Governance Plan.
2. Scope
    a. This policy is applicable to all employees, temporary employees, and contractors of the School. This policy is designed to ensure only authorized disclosure of confidential information. In accordance with School policy and procedures, this policy will be reviewed and adjusted as needed. This Maeser Data Governance Plan works in conjunction with the school Technology Security Policy.
3. Data Privacy & IT Security Staff
    a. Maeser shall appoint, in writing, school Student Data and IT Security Managers responsible for overseeing School-wide data privacy, to include development of School policies and adherence to the standards defined in this document and the School's Technology Security Policy.
4. Responsibilities of the Student Data Manager
    a. Act as the primary local point of contact for the State Student Data Officer.
    b. Create and maintain a list of all LEA staff that have access to personally identifiable student data.
    c. Ensure annual LEA-level training on data privacy to all staff members, including any volunteers with a legitimate need to access student data. Document all staff names, roles, and training dates, times, locations, and agendas.
    d. Provide an annual report to the School's Director and IT Security Manager on employees and contracted partners who have not completed required annual training.
    e. Authorize and manage the sharing, outside of Maeser, of personally identifiable student data from a cumulative record.
5. The student data manager may share personally identifiable student data that are:
    a. of a student with that 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 (except when prohibited in writing by the student's parent)
    h. submitted data requests from external researchers or evaluators
6. The student data manager may not share personally identifiable student data for the purpose of external research or evaluation.
7. Responsibilities of the IT Data Manager
    a. Act as the primary point of contact for the State IT Systems Security Manager.

b. Ensure that all School employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information.
c. Ensure that all students are informed of Cyber Security Awareness.
d. Ensure compliance with security systems laws and Maeser policies and procedures as laid out in the School's Technology Security Policy.
e. Investigate complaints of alleged violations or systems breaches.
f. Provide an annual report to the Maeser board on the School's systems security needs.

8. Employee Non-Disclosure
    a. Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information. All Maeser board members, employees, contractors and volunteers must sign the Maeser Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of State technology and information. Non-compliance with the agreements shall result in consequences up to and including removal of access to the Maeser network; if this access is required for employment, employees and contractors may be subject to dismissal.
9. Disclosure of Personally Identifiable Information
    a. This policy establishes the protocols and procedures for sharing data maintained by Maeser. 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.
10. Student or Student's Parent/Guardian Access
    a. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), Maeser 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. Maeser is not required to provide data that it does not maintain, nor is Maeser required to create education records in response to an eligible student's request.
11. Third Party Vendors
    a. 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). All third-party vendors contracting with Maeser must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401. Vendors determined not to be compliant may not be allowed to enter into future contracts with Maeser without third-party verification that they are compliant with federal and state law, and board rule.
12. Governmental Agency Requests
    a. Maeser 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 of 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, or evaluation.
13. Data Breach
    a. Maeser shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, Maeser staff shall follow industry best practices for responding to the breach and 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.

b. Concerns about security breaches must be reported immediately to the IT Security Manager who will collaborate with appropriate members of the Maeser executive team to determine whether a security breach has occurred. If the Maeser data breach response team determines that one or more employees or contracted partners have substantially failed to comply with Maeser's 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 School's Director.

c. Maeser will provide and periodically update, in keeping with industry best practices, resources for LEA staff, faculty, and volunteers in preparing for and responding to a security breach.

14. Record Retention and Expungement
    a. Maeser 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 Archives and Record Services.
    b. Maeser staff will collaborate with Utah State Archives and Records Services in updating data retention schedules.
15. Expungement Requests
    a. Maeser recognizes the risk associated with retaining student data in perpetuity when such retention could adversely and unfairly affect the relevant student. Maeser shall review all requests for records expungement from parents and make a determination based on the following procedure.
16. Procedure
    a. The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information.
    b. The procedure for expungement shall match the record amendment procedure found in 34 CFR 99, Subpart C of FERPA.
        i. 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.
        ii. Maeser shall decide whether to expunge the data within a reasonable time after the request.
        iii. If Maeser decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
        iv. Maeser shall hold the hearing within a reasonable time after receiving the request for a hearing.
        v. Maeser shall provide the parent notice of the date, time, and place in advance of the hearing.
        vi. The hearing shall be conducted by any individual that does not have a direct interest in the outcome of the hearing.
        vii. Maeser 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.
        viii. Maeser shall make its decision in writing within a reasonable time following the hearing.

ix. The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.

x. If the decision is to expunge the record, Maeser will seal it or make it otherwise unavailable to other staff and educators.

## Appendix A. Maeser Employee Non-Disclosure Agreement

**As an employee of Maeser, I hereby affirm that: (Initial)**

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

_____ I will abide by the terms of Maeser'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 videotape images, of my attempts to access the facility and/or workstations.

**Trainings**

_____ I have completed Maeser's Data Security and Privacy Fundamentals Training ~OR~

_____ I will complete Maeser's Data Security and Privacy Fundamentals Training within 30 days.

**Using Maeser Data and Reporting Systems**

_____ I will use a password-protected computer when accessing data and reporting systems, viewing student/staff records, and downloading reports.

_____ I will not share or exchange individual passwords, for either personal computer(s) or Maeser system user accounts, with Maeser staff or participating program staff.

_____I will log out of and close the browser after each use of Maeser data and reporting systems.

_____I will only access data for 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 school-owned computers.

_____ I will keep any printed files containing personally identifiable information in a locked location while unattended.

_____ I will not share student/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 Maeser server.

**Reporting & Data Sharing**

_____ I will not redisclose or share any confidential data analysis except to other authorized personnel without Maeser's expressed written consent.

_____ I will not publicly publish any data without the approval of the School Director.

_____ 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 or text messages to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email or text message containing such information, I will delete the screenshots/text when forwarding or replying to these messages.

_____I will not transmit student/staff-level data externally unless explicitly authorized in writing.

_____ I understand that when sharing student/staff-identifying data with authorized external individuals, the only approved methods are phone calls or USBE's Secure File Transfer Protocol (SFTP). Sharing within secured server folders or Maeser's Google Drive is appropriate for Maeser 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 Maeser IT Security Manager. Moreover, I acknowledge my role as a public servant and steward of student/staff information, and affirm that I will handle personal information with care to prevent disclosure.

**Consequences for Non-Compliance**

_____ I understand that my access to the Maeser network and systems can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information;

_____ I understand that violation of this confidentiality may subject me to personnel action, including termination;

_____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 Maeser, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of Maeser without the prior written permission of the Student Data Manager of Maeser.

Print Name: _____

Signed: _____

Date: _____