Guadalupe Agency Data Governance Plan

1.1 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. Guadalupe School 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 Guadalupe Agency *Board of Directors* create and implement a policy titled 'Data Governance Plan'.

1.2 SCOPE AND APPLICABILITY

Guadalupe Agency (Agency) Data Governance Plan (Plan) is applicable to all employees, temporary employees, and contractors of the Agency, including those at Guadalupe School. The Plan is used to assess agreements made to disclose data to third-parties, assess the risk of conducting business, and to ensure only authorized disclosure of confidential information. The Agency governing board will review and adjusted its Plan on an annual basis or more frequently, as needed. The following 8 subsections provide data governance policies and processes:

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 Plan works in conjunction with the Agency Information Security Policy, which:

- Designates Guadalupe School as the steward for all confidential information for students in grades K - 6.
- Designates Data Stewards access for all confidential information.
- Requires Data Stewards to maintain a record of all confidential information that they are responsible for.
- Requires Data Stewards to manage confidential information according to this Plan 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 Plan, the legal, regulatory, or contractual obligation shall take precedence.
- Provides the authority to design, implement, and maintain privacy procedures meeting Agency standards concerning the privacy of data in motion, at rest, and processed by related information systems.
- Ensures that all Agency and Guadalupe School governing 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.

2 DATA ADVISORY GROUPS

2.1 STRUCTURE & MEMBERSHIP

The Agency has a data advisory team, which consists of Agency leadership who have responsibility for providing data to internal and external stakeholders as indicated by the Executive Director.

2.2 INDIVIDUAL AND GROUP RESPONSIBILITIES

The following tables outline individual staff and advisory group responsibilities.

Role	Responsibilities
Guadalupe School Student Data Manager	1. May authorize and manage the sharing of personally identifiable student data, from a cumulative record, to internal and external stakeholders; 2. Act as the primary local point of contact for the state student data officer; 3. May share personally identifiable student data that are: a. of 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, and h. 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. Create and maintain a list of school staff who have access to personally identifiable student data; and 6. Ensure annual training on data privacy during contract week to all staff and volunteers and document names, roles, date, time, location, and agenda.

IT Systems Security Manager	1. Act as the primary point of contact for state student data security administration in assisting the USBE to administer this part; 2. Ensure compliance with security systems laws throughout the public education system, including: a. providing training and support to applicable Guadalupe School employees; and b. producing resource materials, model plans, and model forms for Agency systems security; 3. Investigate complaints of alleged violations of systems breaches; and 4. Provide an annual report to the Agency governing board on Guadalupe School's systems security needs
Executive Director	1. Act as the primary point of contact for external research questions; and 2. Direct staff who provide reports for internal stakeholders

3 EMPLOYEE NON-DISCLOSURE ASSURANCES

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

3.1 SCOPE

All Agency and Guadalupe School governing board members, employees, contractors, and volunteers must sign and follow the Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of Agency and state technology and information.

3.2 NON-COMPLIANCE

Non-compliance will result in consequences up to and including removal of access to the Agency network; if this access is required for employment, employees and contractors may be subject to dismissal.

3.3 NON-DISCLOSURE ASSURANCES

All student data collected ad utilized by the Agency is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This section outlines the way Agency staff utilizes data and protects personally identifiable and confidential information. A signed agreement form is required from all *Agency* staff to verify agreement to adhere to/abide by these practices and will be maintained in Human Resources. All Agency employees and contractors will:

1. Complete a Security and Privacy Fundamentals Training.
2. Consult with the Executive Director and Principal when creating or disseminating reports containing data.
3. Use password-protected, authorized computers when accessing any student-level or staff-level records.
4. NOT share passwords for personal computers or data systems with anyone.
5. Log out of any data system and close the browser after each use.

6. Store sensitive data on appropriate-secured location. Unsecured access and removable storage media, or personally owned computers or devices, are not deemed appropriate for storage of sensitive, confidential, or student data.
7. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided when disposing of such records.
8. NOT share personally identifying data during public presentations.
9. Redact any personally identifiable information when sharing sample reports with general audiences found in Appendix B (Protecting PII in Public Reporting).
10. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
11. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
12. 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.
13. NOT transmit student/staff-level data externally unless expressly authorized by the Executive Director and then only transmit data via approved methods.
14. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

3.4 DATA SECURITY AND PRIVACY TRAINING

Guadalupe School provides training for all Agency staff, including volunteers, contractors, and temporary employees with access to student educational data or confidential educator records, to minimize the risk of human error and misuse of information. Training is provided during contract week and attendees must sign the Acceptable use agreement and Non-disclosure assurances upon completion to receive access to the Agency network and technology. The Guadalupe School Student Data Manager records the names and roles of attendees, as well as the date, time, location, and agenda from the training.

4 DATA DISCLOSURE

4.1 PURPOSE

Providing data to persons and entities outside of the Agency increases transparency, promotes education in Utah, and increases knowledge about Utah public education. This section establishes the protocols and procedures for sharing data maintained by the Agency. 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.

4.2 Procedures for disclosure of Personally Identifiable Information (PII)

4.2.1 Student or Student's Parent/Guardian Access

In accordance with FERPA regulations 20 U.S.C. § 1232g (a) (1) (A) (B) (C) and (D), the Agency programs and Guadalupe School will provide parents with access to their student'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 30 days of receiving an official request. The Agency programs and Guadalupe School is not required to provide data that it does not maintain, nor create education records in response to an eligible student's request.

4.2.2 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 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 Agency programs or Guadalupe School without third-party verification that they are compliant with federal and state law and board rule.

4.2.3 Governmental Agency Requests

Agency programs and Guadalupe School 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 (a) reporting requirement, (b) audit, or (c) evaluation.

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

4.3 Procedure for External disclosure of Non-PII

The Agency may consider 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. The Agency has three levels of data requests based on risk: Low, Medium, and High. The Executive Director will make final determinations on classification of student data requests risk level.

4.3.1 Low-Risk Data Request Process

Definition: High-level aggregate data
Examples:

- Enrollment/participation numbers by program
- Percent of students returning to the Agency program or Guadalupe School the subsequent year

Process: Requester completes external research form and submits it to the Executive Director's Office.

4.3.2 Medium-Risk Data Request Process

Definition: Aggregate data, but because of potentially low n-sizes, the data must have disclosure avoidance methods applied

Examples:

- Enrollment/participation numbers by program and grade/age
- Percent of third-graders scoring proficient on the SAGE ELA assessment
- Child Nutrition Program Free or Reduced Lunch percentages

Process: Requester completes external research form and submits it to the Executive Director's Office.

4.3.3 High-Risk Data Request Process

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

Examples:

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

Process: Requester completes external research form and submits it to the Executive Director's Office.

4.4 Data Disclosure to a Requesting External Researcher or Evaluator

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

The Agency may not disclose PII 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 researchers or evaluators for projects unrelated to federal or state requirements if:

1. The Agency 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 Executive Director.
3. Researchers and evaluators supply the Agency a copy of any publication or presentation that uses Agency data 10 business days prior to any publication or presentation.

Process: Requester completes external research form and submits it to the Executive Director's Office.

5 Data breach

5.1 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.

5.2 PROCEDURES

The Agency follows industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of PII, Agency staff will follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, the Agency follows 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 data advisory team to determine whether a security breach has occurred. If the Agency data advisory team determines that one or more employees or contracted partners have substantially failed to comply with 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 Executive Director.

The Agency will provide and periodically update, in keeping with industry best practices, resources for staff, contractors, and volunteers in preparing for and responding to a security breach.

6 RECORD RETENTION AND EXPUNGEMENT

6.1 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.

6.2 PROCEDURE

Agency staff retains and dispose of student records in accordance with Section 63G-2-604, 53A-1-1407, and complies with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with 53A-1-1407, Agency programs and Guadalupe School will expunge student data that is stored upon request of the student if the student is at least 23 years old. Agency programs and Guadalupe School may expunge medical records and behavioral test assessments. Agency programs and Guadalupe School will not expunge student records of grades, transcripts, a record of the student's enrollment, or assessment information. Agency program and Guadalupe School staff will collaborate with Utah State Achieves and Records Services, USBE, and contractors with expert knowledge in updating data retention schedules.

Agency program and Guadalupe School maintained student-level discipline data will be expunged three years after the data is no longer needed.

7 QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS

7.1 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:

7.1.1 Data Governance Structure

The Plan is structured to encourage the effective and appropriate use of educational data. The *Plan* centers on the idea that data is the responsibility of all program staff 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.

7.1.2 Data Requirements and Definitions

Clear and consistent data requirements and definitions are necessary for good data quality. On the data collection side, the Agency receives training from and regularly communicates with the USBE regarding data requirements and definitions.

7.1.3 Data Auditing

The data advisory team and Principal perform regular and ad hoc data auditing. They analyze data for anomalies, investigate the source of the anomalies, and correct the anomalies, as appropriate.

7.1.4 Quality Control Checklist

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

8 DATA TRANSPARENCY

Annually, *Guadalupe School* will publically post:

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

9 APPENDIX

Appendix A. Agency Employee Non-Disclosure Agreement

As an employee of the Guadalupe Agency, I hereby affirm that: (Initial)

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

_____ I will abide by the terms of Agency's Data Governance Plan and corresponding plans, processes, 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 Guadalupe Agency's Data Security and Privacy Fundamentals Training.

Using Guadalupe Agency 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 *Agency* user accounts, with *anyone*.

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

_____I will only access data in which I have received permission to use in order to fulfill job duties.

_____I will not attempt to identify individuals with the data, except as is required to fulfill job or volunteer duties.

Handling Sensitive Data

_____ I will keep sensitive data on password-protected, authorized computers.

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

_____ I will not share student/staff-identifying data during public presentations.

_____ I will delete files containing sensitive data after working with them from my desktop or local computer drives.

Reporting & Data Sharing

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

_____ I will take steps to avoid disclosure of PII in 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 student/staff-level data externally unless explicitly authorized by the Executive Director.

_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the Executive Director. 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 access to the Agency network and systems can be suspended based on any violation of this agreement 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 the Agency, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone without the prior written permission of the Executive Director.

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 Agency programs and Guadalupe School is comprehensive, the data made available to the public is masked to avoid unintended disclosure of PII in 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. 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 Agency employee 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