Merit Preparatory Academy Data Governance Plan

1. Governing Principles

Merit Preparatory Academy (referred to as the LEA throughout) takes its responsibility toward student data seriously. This governance plan incorporates the following Generally Accepted Information Principles (GAIP):

- **Risk:** There is risk associated with data and content. The risk must be formally recognized, either as a liability or through incurring costs to manage and reduce the inherent risk.
- **Due Diligence:** If a risk is known, it must be reported. If a risk is possible, it must be confirmed.
- **Audit:** The accuracy of data and content is subject to periodic audit by an independent body.
- **Accountability:** An organization must identify parties which are ultimately responsible for data and content assets.
- **Liability:** The risks in information means there is a financial liability inherent in all data or content that is based on regulatory and ethical misuse or mismanagement.

2. Data Maintenance and Protection Policy

The LEA recognizes that there is risk and liability in maintaining student data and other education-related data and will incorporate reasonable data industry best practices to mitigate this risk.

2.1 Process

In accordance with R277-487, the LEA shall do the following:

- Designate an individual as an Information Security Officer
- Adopt the CIS Controls or comparable
- Report to the USBE by October 1 each year regarding the status of the adoption of the CIS controls or comparable and future plans for improvement.

3. Roles and Responsibilities Policy

The LEA acknowledges the need to identify parties who are ultimately responsible and accountable for data and content assets. These individuals and their responsibilities are as follows:

3.1 Data Manager roles and responsibilities

- authorize and manage the sharing, outside of the student data manager's education entity, of personally identifiable student data for the education entity as described in this section
- provide for necessary technical assistance, training, and support
- act as the primary local point of contact for the state student data officer
- ensure that the following notices are available to parents:
    - annual FERPA notice (see 34 CFR 99.7),
    - directory information policy (see 34 CFR 99.37),
    - survey policy and notice (see 20 USC 1232h and 53E-9-203),

- data collection notice (see 53E-9-305)

3.2 Information Security Officer

- Oversee adoption of the CIS controls
- Provide for necessary technical assistance, training, and support as it relates to IT security

4. Training and Support Policy

The LEA recognizes that training and supporting educators and staff regarding federal and state data privacy laws is a necessary control to ensure legal compliance.

4.1 Procedure

1. The data manager will ensure that educators who have access to student records will receive an annual training on confidentiality of student data to all employees with access to student data. The content of this training will be based on the Data Sharing Policy.
2. By October 1 each year, the data manager will report to USBE the completion status of the annual confidentiality training and provide a copy of the training materials used.
3. The data manager shall keep a list of all employees who are authorized to access student education records after having completed a training that meets the requirements of 53E-9-204.

5. Audit Policy

In accordance with the risk management priorities of the LEA, the LEA will conduct an audit of:

- The effectiveness of the controls used to follow this data governance plan; and
- Third-party contractors, as permitted by the contract described in 53E-9-309(2).

6. Data Sharing Policy

There is a risk of redisclosure whenever student data are shared. The LEA shall follow appropriate controls to mitigate the risk of redisclosure and to ensure compliance with federal and state law.

6.1 Procedure

1. The data manager shall approve all data sharing or designate other individuals who have been trained on compliance requirements with FERPA.
2. For external research, the data manager shall ensure that the study follows the requirements of FERPA's study exception described in 34 CFR 99.31(a)(6).

After sharing from student records, the data manager shall ensure that an entry is made in the LEA Metadata Dictionary to record that the exchange happened.

3. After sharing from student records, the data manager shall make a note in the student record of the exchange in accordance with 34 CFR 99.32.

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.

1. 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.
2. The LEA shall decide whether to expunge the data within a reasonable time after the request.
3. 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.
4. The LEA shall hold the hearing within a reasonable time after receiving the request for a hearing.
5. The LEA shall provide the parent notice of the date, time, and place in advance of the hearing.
6. The hearing shall be conducted by any individual that does not have a direct interest in the outcome of the hearing.
7. 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.
8. The LEA shall make its decision in writing within a reasonable time following the hearing.
9. The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.
10. If the decision is to expunge the record, the LEA will seal it or make it otherwise unavailable to other staff and educators.

8. Data Breach Response Policy

The LEA shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, the LEA staff shall follow industry best practices for responding to the breach.

8.1 Procedures

1. The director will work with the information security officer to designate individuals to be members of the cyber incident response team (CIRT)
2. At the beginning of an investigation, the information security officer will begin tracking the incident and log all information and evidence related to the investigation.
3. The information security officer will call the CIRT into action once there is reasonable evidence that an incident or breach has occurred.
4. The information security officer will coordinate with other IT staff to determine the root cause of the breach and close the breach.

5. The CIRT will coordinate with legal counsel to determine if the incident is meets the legal definition of a significant breach as defined in R277-487 and determine which entities and individuals need to be notified.
6. If law enforcement is notified and begins an investigation, the CIRT will consult with them before notifying parents or the public so as to not interfere with the law enforcement investigation.

9. Publication Policy

The LEA recognizes the importance of transparency and will post this policy on the LEA website.