DATA GOVERNANCE PLAN

GOVERNING PRINCIPLES

American Leadership 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.

DATA MAINTENANCE AND PROTECTION

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.

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.

ROLES AND RESPONSIBILTIES

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:

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)

Information Security Officer

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

TRAINING AND SUPPORT

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.

Procedure

1. All LEA employees, and contracted partners must sign and follow the Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.
2. 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.
3. 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.
4. 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.

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).

DATA SHARING

Providing data to persons and entities outside of American Leadership Academy 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 American Leadership Academy. 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.

DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

The data manager shall approve all data sharing or designate other individuals who have been trained on compliance requirements with FERPA.

1. Student or Student's Parent/Guardian Access: Parents are advised that access to their student's record can be obtained from the student's school. 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. ALA is not required to provide data that it does not maintain.
2. School Officials Access: School officials who have a legitimate educational interest in a student's education record may access the record without parental consent. For the purpose of this Plan, "school officials" shall mean any employees, trustees, or agents of the school, or of facilities with which the school contracts for placement of students with disabilities. The term also

includes attorneys, consultants, and independent contractors who are retained by the school, or by facilities with which the school contracts for placement of students with disabilities. School officials have a legitimate educational interest in a student's records when they are working with the student, considering disciplinary or academic actions, reviewing an individualized education program (IEP) for a student with disabilities, compiling statistical data, or investigating or evaluating programs that may involve the student.

3. Access by Other Persons: Personally identifiable information in education records shall not be released, except to the following:
    - Individuals for whom the parent has given written consent. Parents should use the District Consent to Release Educational Records of Student form.
    - School officials, including teachers, who have legitimate educational interests.
    - Officials of other schools, school systems, or institutions of postsecondary education in which the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer.
    - Authorized representatives of the Comptroller General of the United States, the Secretary of Education, or state and local educational authorities who require access to student or other records necessary in connection with the audit and evaluation of federal or state supported education programs or in connection with the enforcement of or compliance with federal legal requirements that relate to such programs.
    - Personnel involved with the student's application for, or receipt of, financial aid.
    - Organizations conducting studies for educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction. Such studies must be conducted so that personal identification of students and their parents will not be revealed to persons other than authorized personnel of the organizations conducting the studies.
    - Accrediting organizations that require the information for purposes of accreditation.
    - Parents of a student who is a dependent for tax purposes.
    - The student.
    - Individuals authorized by a judicial order or lawfully issued subpoena.
    - Appropriate persons who, in an emergency, must have such information in order to protect the health or safety of the student or other person.
    - Persons or organizations authorized by the school's administration to obtain directory information.
    - An agency caseworker or other representative of a state or local child welfare agency who provides documentation showing the right of that caseworker or representative to access the particular student's case plan. If shared with the Department of Human Services, the Department must be legally responsible for the care and protection of the student or providing services to the student. The student's PII may not be shared with a person who is not authorized to address the student's education needs. Consistent with UTAH CODE ANN. § 53E-9-308(4) (2018), a school official may share personally identifiable student data to improve education outcomes for youth:
4. 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).

5. 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.

EXPUNGEMENT REQUEST

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.

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.

DATA BREACH RESPONSE

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.

PROCEDURES

1. The Executive 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.

PUBLICATION POLICY

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