DATA GOVERNANCE PLAN

PURPOSE

American Leadership Academy takes seriously it moral and legal responsibility to protect student data privacy and ensure student data security. The School is required by Utah's Student Data Protection Act and the School's Student Data Privacy and Security Policy to establish a Data Governance Plan.

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.

SCOPE AND APPLICABILITY

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

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

In addition, this Plan works in conjunction with the School's Information Technology Security Plan which provides policies and processes for:

1. Systems administration
2. Network security
3. Application security
4. Server and device security
5. Identity, authentication, and access management
6. Data protection
7. Acquisition and asset management
8. Training

DATA ADVISORY TEAM

The School has a data advisory team, which consists of those having responsibility for providing data to internal and external stakeholders as appointed by the Director.

STUDENT DATA MANAGER

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's student data officer.
3. May share personally identifiable student data that is:
    a. about a student with that student and/or that 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 a response to a subpoena issued by a court;
    g. directory information; or
    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 staff that have access to personally identifiable student data.
6. Ensure all staff members, including volunteers, receive annual level training on data privacy. Document all staff names, roles, and training dates, times, locations, and agendas.
7. Ensure that the School's metadata dictionary is created, maintained, published, and provided to the Utah State Board of Education as required by law.

IT SYSTEMS SECURTIY MANAGER

The School's contracted IT provider will function as the School's IT Security Manager. The IT Security Manager's responsibilities include the following:

1. Acts as the primary point of contact for state student data security administration.
2. Ensures compliance with security systems laws throughout the public education system.
3. Assist in training and support to employees on IT security matters.
4. Investigates complaints of alleged violations of systems breaches.
5. Provide an annual report to the board on the systems security needs.

EMPLOYEE NON-DISCLOSURE ASSURANCES

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

All American Leadership Academy board members, employees, contractors and volunteers, who have access to education records, must sign and obey the ALA Employee Non-Disclosure Agreement 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 ALA network; if this access is required for employment, employees and contractors may be subject to dismissal.

EMPLOYEES NON-DISCLOSURE ASSURANCES

All student data utilized by ALA is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all ALA staff to verify agreement to adhere to/abide by these practices. These responsibilities with respect to student data privacy and security include:

1. Participating in student data privacy training each year as required by the School.
2. Sign a statement each year certifying completion of student data privacy training and understanding of student data privacy requirements as required by the School (not required by volunteers).
3. Not sharing personally identifiable student data outside of the School unless authorized to do so by law and the Student Data Manager.
4. Using password-protected School-authorized computers when accessing the School's data systems or viewing or downloading any student-level records.
5. Not sharing or exchanging individual passwords for School-authorized computers or School data systems.
6. Logging out of any School data system or portal and closing the browser after each use or extended absence.
7. Store sensitive data in appropriately secured locations. Unsecured flash drives, DVDs, CD-ROMs 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 documents with personally identifiable student data in a locked, secured location and use School-approved document destruction methods when disposing of such records.
9. Not sharing personally identifiable student data during public presentations.
10. Using secure methods when sharing or transmitting personally identifiable student data with authorized individuals.
11. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, etc.
12. Only accessing and using student data as authorized by the School to fulfill job or volunteer duties, and not for any other purpose.
13. Not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information.
14. Use secure methods when sharing or transmitting sensitive data. The approved method for external transfer is the USBE Secure File Transfer Protocol (SFTP) website. Sharing within the ALA Google Drive is appropriate for internal file transfer.
15. Consult with the Student Data Manager regarding any questions about personally identifiable student data and related privacy laws, requirements, or concerns.
16. Limit use of individual data to the purposes which have been authorized with the scope of job responsibilities.

DATA SECURITY AND PRIVACY TRAINING

American Leadership Academy will provide training opportunities for all 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.

1. All American Leadership Academy employees, and contracted partners must sign and follow the Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.
2. New employees that do not comply may not be able to use ALA networks or technology.
3. All current employees and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum.
4. USBE requires a targeted Security and Privacy Training for Data Stewards and IT staff, to facilitate providing training for other specific groups within each School that collect, store, or disclose data.
5. Participation in training, as well as a signed copy of the Employee Non-Disclosure Agreement, will be annually monitored by the School's Director.

DATA DISCLOSURE

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)

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. Third Party Vendors: 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 ALA 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 ALA without third-party verification that they are compliant with federal and state law, and board rule.

3. Internal Partner Requests: Internal partners to USBE include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in USBE's data request ticketing system.
4. Governmental Agency Requests: ALA 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.

DATA BREACH

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.

ALA shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, ALA staff shall follow industry best practices for responding to the breach. Further, ALA 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 ALA administrative team to determine whether a security breach has occurred. Failure to comply with relevant privacy policies, will lead to appropriate consequences, which may include termination of employment or a contract and further legal action. Concerns about security breaches that involve the IT Security Officer must be reported immediately to the School's Director.

RECORD RETENTION AND EXPUNGEMENT

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

ALA 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. In accordance with 53A-1-1407, ALA shall expunge stored student data upon request of the student if the student is at least 23 years old. ALA may expunge medical records and behavioral test assessments. ALA will not expunge student records of grades, transcripts, records of the student's enrollment, or assessment information. ALA staff will collaborate with Utah State Archives and Records Services in updating data retention schedules. ALA-maintained student-level discipline data will be expunged after three years.

QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS

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 is addressed in five areas:

1. Data Governance Structure: The ALA data governance plan is structured to encourage the effective and appropriate use of educational data. The ALA data governance structure centers on the idea that data is the responsibility of all ALA sections 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.
2. Data Requirements and Definitions: Clear and consistent data requirements and definitions are necessary for good data quality. On the data collection side, the Utah State Board of Education communicates data requirements and definitions to LEAs through the Data Clearinghouse Update Transactions documentation (see http://www.schools.utah.gov/computerservices/Data-Clearinghouse.aspx). Data Stewards coordinate data releases through the Data Stewards Group meetings. All data released includes relevant data definitions, business rules, and are date stamped. Further, Data and Statistics produces documentation, trainings and FAQs on key statistics and reports, such as AYP, graduation rate and class size.
3. Data Collection: Data elements should be collected only once—no duplicate data collections are permitted. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data. For all new data collections, the USBE provides to LEAs clear guidelines for data collection and the purpose of the data request. The USBE also notifies LEAs as soon as possible about future data collections. Time must be given to LEAs in order for them to begin gathering the data needed.
4. Data Auditing: Data and Statistics Data Analysts perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with IT and/or LEAs in explaining and/or correcting the anomalies. Data Analysts also work with School Finance to address findings from the Auditors.

DATA TRANSPARENCY

Annually, American Leadership Academy will publicly post:

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