Athlos Academy of Utah Data Governance Plan

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. Athlos Academy of Utah (AAU) 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 AAU adopt a Data Governance Plan.

2 SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, volunteers, and contractors of the school. The policy must be used to assess agreements made to disclose data to third-parties. In accordance with school policy and procedures, this policy will be reviewed and adjusted on an annual basis or more frequently, as needed. This policy is designed to ensure only authorized disclosure of confidential information. The following 8 subsections provide data governance policies and processes for AAU:

1. Roles and Responsibilities
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 AAU Data Governance Plan works in conjunction with policies *4004 – Employee Records*, *5105 – Student Records Protection*, *5108 – Student Directory Information*, *5402 – Electronic Devices*, *7401 – Acceptable Use of Technology*, *7402 – Technology Security, 8008 – Access to Private Data*, and *8009 – External Research Requests*.

3 ROLES AND RESPONSIBILITIES

3.1 INDIVIDUAL RESPONSIBILITIES

The following tables outlines individual AAU staff responsibilities.

Role	Responsibilities

LEA Student Data ManagerData Manager	1. Authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity 2. Act as the primary local point of contact for the state student data officer. 3. A Data Manager 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 h. submitted data requests from external researchers or evaluators, 4. A Data Manager may not share personally identifiable student data for the purpose of external research or evaluation. 5. Create and maintain a list of all AAU staff that have access to personally identifiable student data. 6. Ensure annual school-level training on data privacy to all staff members, including volunteers. Document all staff names, roles, and training dates, times, locations, and agendas.
IT Security Manager	1. Acts as the primary point of contact for state student data security staff. 2. Ensures compliance with school policies, including *7402 – Technology Security*. 3. Ensures that staff receive adequate training and support to follow this plan and related policies. 4. Investigates complaints of alleged violations of systems breaches. 5. Ensures that periodic audits are conducted of this and the Technology Security Plan. 6. Provides input into the annual review of this plan. 7. Provides an annual report to the board on AAU's systems security needs, if needed.

3.1.1 Table 1. Individual *AAU* Staff Responsibilities

3.2 INDIVIDUAL IDENTIFICATION

Unless otherwise designated by the governing board, the School Leader shall act as the Data ManagerLEA Student Data Manager for AAU. The School Leader shall appoint an IT Security Security Manager.

4 EMPLOYEE NON-DISCLOSURE ASSURANCES

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

4.1 SCOPE

All AAU board members, employees, contractors and volunteers must sign and obey the AAU Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of school technology and information.

4.2 NON-COMPLIANCE

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

4.3 NON-DISCLOSURE ASSURANCES

All student data utilized by AAU is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way AAU staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all AAU staff to verify agreement to adhere to/abide by these practices and will be maintained by Human Resources. All AAU employees (including contract or temporary) will:

1. Complete a Security and Privacy Fundamentals Training.
2. Complete a Security and Privacy Training for Researchers and Evaluators, if your position is a research analyst or if requested by the Chief Privacy Officer.
3. Consult with AAU internal data owners when creating or disseminating reports containing data unless exempted by state or federal law.
4. Use password-protected school-owned computers when accessing any student-level or staff-level records.
5. Not share individual passwords for computers or data systems with anyone.
6. Log out of any data system/portal and close the browser after each use.
7. Store sensitive data on appropriate-secured location. Unsecured access flash drives, DVD, CD-ROM 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 reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at AAU when disposing of such records.
9. Not share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used for such presentations.
10. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager, found in Appendix B (Protecting PII in Public Reporting).

11. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
12. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
13. 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 Manager should be consulted.
14. Use secure methods when sharing or transmitting sensitive data, such as a Secure File Transfer Protocol (SFTP) website. Also, sharing within secured server folders is appropriate for AAU internal file transfer.
15. Not transmit child/staff-level data externally unless expressly authorized in writing by the data owner or otherwise allowed under state/federal law and then only transmit data via approved methods such as described in item ten.
16. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

4.4 DATA SECURITY AND PRIVACY TRAINING

4.4.1 Purpose

AAU will provide a range of training opportunities for all AAU 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.

4.4.2 Scope

All AAU board members, employees, volunteers, and contracted partners.

4.4.3 Compliance

New employees that do not comply may not be able to use AAU networks or technology.

4.4.4 Policy

1. Within the first week of employment, all AAU board members, employees, and contracted partners must sign and follow the AAU Employee Acceptable Use Policy, which describes the permissible uses of school technology and information.
2. New employees that do not comply may not be able to use AAU networks or technology. Within the first week of employment, all AAU board members, employees, and contracted partners also must sign and obey the AAU Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current AAU board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 60 days of the adoption of this rule.

4. AAU requires a targeted Security and Privacy Training for Data ManagerData Managers and IT staff for other specific groups within the school that collect, store, or disclose data.
5. Participation in the training as well as a signed copy of the Employee Non-Disclosure Agreement will be annually monitored by the School Leader. The School Leader will annually report any AAU board members, employees, and contracted partners who do not have these requirements completed to the IT Security Manager.

5 DATA DISCLOSURE

5.1 PURPOSE

Providing data to persons and entities outside of AAU increases transparency, informs key stakeholders of school performance, and allows AAU to consult with experts to improve instructional outcomes. This policy establishes the protocols and procedures for sharing data maintained by AAU. 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.

5.2 POLICY FOR DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

5.2.1 Student or Student's Parent/Guardian Access

Parents are advised that the records maintained by AAU consist of data generated through the course of providing educational services to students as well as data provided to AAU by parents and by the school district in which their student was previously enrolled. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), AAU 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. AAU is not required to provide data that it does not maintain, nor is AAU required to create education records in response to an eligible student's request. More information on parent/guardian access can be found in *Community Relations Policy 8008 – Access to Private Data*

5.2.2 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 contracting with AAU 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 AAU without third-party verification that they are compliant with federal and state law, and board rule.

5.2.3 Governmental Entity Requests

AAU 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 entity must provide evidence 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
c) evaluation

The Data Manager will ensure the proper data disclosure avoidance is included if necessary. An InteragencyAgreement must be reviewed by legal staff and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."

5.3 Policy for External disclosure of Non-Personally Identifiable Information (PII)

5.3.1 Scope

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.

5.3.2 Student Data Disclosure Risk Levels

AAU has determined three levels of data requests with corresponding policies and procedures for appropriately protecting data based on risk: Low, Medium, and High. The Data Manager will make final determinations on classification of student data requests risk level.

5.3.2.1 Low-Risk Data Request Process

Definition: High-level aggregate data
Examples:

- Graduation rate by year for the state
- Percent of third-graders scoring proficient on the SAGE ELA assessment

Process: Request is forwarded to appropriate Data Manager. Data Manager fulfills request and saves the dataset in a secure folder.

5.3.2.2 Medium-Risk Data Request Process

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

Examples:

- Graduation rate by year and LEA
- Percent of third-graders scoring proficient on the SAGE ELA assessment by school
- Child Nutrition Program Free or Reduced Lunch percentages by school

Process: Request is forwarded to appropriate Data Manager, Data Manager fulfills request, applies appropriate disclosure avoidance techniques, and data are sent to requester. The Data Manager saves

the dataset in a secure folder.

5.3.2.3 High-Risk Data Request Process

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

Examples:

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

Process: Request is sent to the Data Manager. If the request is approved and no agreement exists between AAU and the requesting party allowing transfer of this information, an MOA is drafted and sent to legal, placed on the board consent calendar. If approved, the appropriate Data Manager fulfills request, de-identifies data as appropriate, sends to requester, and saves the dataset in a secure folder.

5.4 Data Disclosure to a Requesting External Researcher or Evaluator

Requests for data from external researchers or evaluators shall to processed according to *Community Relations Policy 8009 – External Research Requests*.

6 Data breach

6.1 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.

6.2 Policy

AAU shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, AAU staff 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 AAU administrative team to determine whether a security breach has occurred. If the administrative team determines that one or more employees or contracted partners have substantially failed to comply with AAU's Technology 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 Leader.

7 RECORD RETENTION AND EXPUNGEMENT

7.1 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.

7.2 SCOPE

AAU board members and staff.

7.3 POLICY

AAU 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 Archive and Record Services.

8 QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS

8.1 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:

8.1.1 Data Governance Structure

The AAU data governance plan is structured to encourage the effective and appropriate use of educational data. The AAU data governance structure centers on the idea 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.

8.1.2 Data Requirements and Definitions

Clear and consistent data requirements and definitions are necessary for good data quality. AAU shall collect data in accordance with the Data Clearinghouse Update Transactions documentation from USBE

8.1.3 Data Collection

Data elements should be collected only once whenever possible. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level).

8.1.4 Data Auditing

AAU staff shall perform regular and ad hoc data auditing. They shall analyze for anomalies, investigate the source of the anomalies, and work with IT school staff in explaining and/or correcting the anomalies. The Data Manager will also work with School Finance to address findings from the Auditors.

8.1.5 Quality Control Checklist

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

9 DATA TRANSPARENCY

Annually, *AAU* will publicly post:

- This plan;
- Relevant data policies; and
- A Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401

10 APPENDIX

Appendix A. *AAU* Employee Non-Disclosure Agreement

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

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

_____ I will abide by the terms of the *AAU*'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 your attempts to access the facility and/or workstations.

Trainings

_____ I have completed *AAU*'s Data Security and Privacy Fundamentals Training.

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

Using AAU Data and Reporting Systems

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

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

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

_____I will only access data in 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 state-authorized computers.

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

_____ I will not share child/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 *AAU* server.

Reporting & Data Sharing

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

_____ I will not publicaly publish any data without the approval of the Superintendent.

_____ 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 <u>not</u> 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 child/staff-level data externally unless explicitly authorized in writing.

_____ I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or *AAU*'s Secure File Transfer Protocol (SFTP). Also, sharing within secured server folders is appropriate for *AAU* 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 *AAU* Information Security Officer. Moreover, I acknowledge my role as a public servant and steward of child/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 *AAU* network and systems can be suspended based on any violation of this contract 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 *AAU*, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of *AAU* without the prior written permission of the Student Data Manager of *AAU*.

Print Name: _____

Signed: _____

Date: _____

Appendix B. Protecting PII in Public Reporting

Data Gateway Statistical Reporting Method for Protecting PII

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 the *AAU* (*AAU*) and local education agencies (LEAs) is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school, LEA, or state-level 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. Example 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 Data Manager 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