Tuacahn High School Data Governance Plan

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. Tuacahn High School for the Arts (THSA) 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 THSA adopt a Data Governance Plan.

Scope and Applicability:
This policy is applicable to all employees, temporary employees, and contractors of the high school. The policy must be used to assess agreements made to disclose data to third parties. This policy must also be used to assess the risk of conducting business. In accordance with THSA 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 THSA.

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 THSA Data Governance Plan works in conjunction with the Agency Information Security Policy, which:
Designates THSA as the steward for all confidential information maintained with THSA,
Designates Data Stewards to maintain a record of all confidential information that we are responsible for:
Requires Data Stewards to manage confidential information according to this policy and all other applicable policies, standards and plans;
Complies with all legal, regulatory and contractual obligations regarding privacy of THSA data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence;
Provides the authority to design, implement, and maintain privacy procedures meeting THSA standards concerning the privacy of data in motion, at rest and processed by related information systems;
Ensures that all THSA 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 cryptology

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.

Data Advisory Groups:
THSA has a three-tiered data governance structure to ensure that data is protected at all levels of Utah's educational system.

Membership in the groups require board approval. Group membership is for two years. If individual members exit the group prior to fulfilling their two-year appointment, the board may authorize THSA's Principal to appoint a replacement member.

The following outlines THSA's staff and advisory group responsibilities.

LEA Student Data 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 student data manager may share personally identifiable student date that is: 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 the 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 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 student data manager may not share personally identifiable student data for the purposed of external research or evaluation 5. Create and maintain a list of all LEA staff that have access to personally identifiable student data 6. Ensure annual LEA training on data privacy to all staff members, including volunteers. Document all staff names, roles., and training dates, times, locations, and agendas
IT Systems Security Manager	1. Acts as the primary point of contact for state student data security administration in assisting the board to administer this part 2. Ensures compliance with security systems laws throughout the public education system, including: a. providing training and support to applicable THSA employees b. producing resource materials, model plans, and model forms for LEA systems security. 3. Investigates complaints of alleged violations of systems breaches 4. Provides an annual report to the board on THSA systems security needs.

Educators	Maintain student privacy and mentor new staff members.
Other	

Organization and roles:

The LEA shall appoint a Student Data Manager and an IT Security Manager, who shall fulfill the roles described in Table 1. As the LEA's data governance matures, a data governance group will be formed, which will oversee compliance with the data governance plan, assess risks, and provide recommendations for controls and other policies related to data governance.

Data governance, security, and privacy are ultimately the responsibility of all employees of the LEA, including educators, who will follow this data governance plan per the guidance and training they receive from the Student Data Manager.

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

Scope:
All THSA board members, employees, contractors and volunteers must sign and obey the THSA Employee Non-Disclosure Agreement (see Appendix A), which describes the permissible uses of state technology and information.

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

Non-Disclosure Assurances:
All student date utilized by THSA is protected as defined by FERPA and Utah statute. This policy outlines the way THSA staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all THSA staff to verify agreement to adhere to/abide by these practices and will be maintained in THSA Human Resources. All THSA employees 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 THSA internal data owners when creating or disseminating reports containing data
4. Use password-protected state-authorized computers when accessing any student level or staff level records
5. NOT share individual passwords for personal 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 and 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 THSA 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
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 authorized users
13. NOT use e-mail to send screenshots, text, or attachments that contain personally identifiable information or other sensitive information. If users receive an e-mail containing such information, they will delete 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
14. Use secure methods when sharing or transmitting sensitive data. The approved method is THSA's Safe Send file transfer method. Also, sharing within secured server folders is appropriate for THSA's internal file transfer
15. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods such as described above
16. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

Data Security and Privacy Training:

Purpose:
THSA will provide training opportunities for all THSA 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.

Scope:
All THSA board members, employees, and contracted partners.

Compliance:
New employees that do not comply may not be able to use THSA networks or technology.

Policy:
1. Within the first week of employment, all THSA board members, employees, and contracted partners must sign and follow the THSA 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 THSA networks or technology. Within the first week of employment, all THSA board members, employees and contracted partners must also sign and obey the THSA Employee Non-Disclosure Agreement, which describes the appropriate uses and the safeguarding of student and educator date.

3. All current THSA board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 90 days of the adoption of this rule.
4. THSA requires a targeted Security and Privacy Training for Data Stewards and IT staff for other specific groups within the agency that collect, store, or disclose data. The Chief Privacy Officer will identify these groups. Data and Statistics Coordinator will determine the annual training topics for these targeted groups based on THSA's training needs.
5. Participation in the training as well as a signed copy of the Employee Non-Disclosure Agreement will be annually monitored by supervisors. Supervisors and the board secretary will annually report all THSA board members, employees, and contracted partners who do not have these requirements complete to the IT Security Manager.

DATA DISCLOSURE:

Purpose:
Providing data to persons and entities outside of THSA 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 THSA. It is intended to be consistent with the disclosure provisions of FERPA, 20 U.S.C. 1232g, 34 CFR part 99, and Utah's Student Data Protection Act (SDPA), U.C.A. 53A-1-1401.

Policy for Disclosure of Personally Identifiable Information (PPI):

Student or Student's Parent/Guardian Access:

Parents are advised that the records maintained by THSA are provided to THSA by the school district in which their student is/was enrolled, and access to their student's record can be obtained from the student's school district. In accordance with FERPA regulations, 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 or parents, and confidential letters of recommendation if the student has waived the right to access), within 45 days of receiving an official request. LEAs and THSA are not required to provide data that it does not maintain, nor is THSA required to create education records in response to an eligible student's request.

Third Party Vendors:

Third party vendors may have access to students' PII if the vendor is designated as a "school official" as defined in FERPA. 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 THSA must be compliant with Utah's Student Data Protection Act. Vendors determined not to be compliant may not be allowed to enter into future contracts with THSA without third-party verification that they are compliant with federal and state law, and board rule.

Internal Partner Requests:

Internal partners to THSA include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in THSA's data request ticketing system.

Governmental Agency Requests:

THSA 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 reporting requirement, audit, or evaluation. The requesting governmental agency 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 coordinator of Data and Statistics will ensure the proper data disclosure avoidance are included if necessary. An Interagency Agreement must be reviewed by legal staff and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."

Data Disclosures

All disclosures of student data must be done in accordance with the Family Educational Rights and Privacy Act (FERPA) and the Utah Student Data Protection Act.

Written parental consent

Data may be disclosed to any party and in any case where the parent or adult student provides written parental consent. Per 34 CFR 99.30, this consent must

- Specify the records that may be disclosed
- State the purpose of the disclosure
- Identify the party or class of parties to whom the disclosure will be made

Parents or adult students may request that a copy of disclosed records be shared with them.

An electronic signature that identifies and authenticates the individual and their approval meets the requirement of written parental consent.

Exceptions where written parental consent is not required

FERPA in 20 USC 1232g and 34 CFR 99.31 and the Utah Student Data Protection Act provide for several cases where the LEA may disclose education records without prior written parental consent. Each exception specifies a different entity that may receive education records and what assurances and restrictions must be followed.

Policy for External Disclosure of Non-PII

Scope:
External data requests from individuals or organizations that are not intending on conduction external research or are not fulfilling a state or federal reporting requirement, audit or evaluation.
Student Data Disclosure Risk Levels:
THSPA has determined four levels of data request with corresponding policies and procedures for appropriately protecting data based on risk: Low, Medium, and High. The Coordinator of Data and Statistics will make final determination on classification of student data requests risk level.

Low-Risk Data Request Process

Definition: High-level aggregate data

Examples:

Graduation rate by year for the state

State required testing

Process: Requester sends the request, Data request forwarded to appropriate Data Steward. Data Steward fulfills request and saves the dataset in a secure folder managed by the Coordinator or Data Statistics. The request is recorded as filled.

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 for the state

State required testing

Economically Disadvantaged percentages

Process: Requester sends request which is forwarded to the appropriate Data Stewart; Data steward fulfills request, applies appropriate disclosure avoidance techniques and sends to another data steward for Quality Assurance (ensuring student data protection). If it passes QA, data is sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. Data Steward closes the request. If it does not pass QA the data is sent back to the Data Steward for modification.

High Risk Data Request Process

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

Examples:

De-identified student-level graduation data

De-identified student-level state required assessment scores

Process: Requester sends request which is sent to Data and Statistic Coordinator for review. If the request is approved, an MOA is drafted and sent to legal, placed on the board consent calendar, reviewed by the Superintendent, sent to the Purchasing/Contract Manager, sent to the Coordinator of Data and Statistics, appropriate Data Steward fulfills request, de-identifies data as appropriate and sends to another Data Steward for Quality Assurance. If it passes QA data is sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The data steward closes the request. If it does not pass QA the data is sent back to the Data Steward for modification.

Data Disclosure to a Requesting External Researcher of Evaluator

Responsibility:

The Coordinator of Data and Statistics will ensure the proper data is shared with external researcher or evaluator to comply with federal, state and board rules.

THSA 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 researcher or evaluators for projects unrelated to federal or state requirements if:

1. THSPA Director, Superintendent or board member sponsors an external researcher or evaluator request
2. Student data is not PII and is de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Coordinator of Data and Statistics
3. Researches and evaluators supply THSPA a copy of any publication or presentation that uses THSPA data 10 business days prior to any publication or presentation.

Process: Research proposal must be submitted using this form: http://www.schools.utah.gov/data/Data-request/ResearcherProposal.aspx. Research proposals are sent directly to the Coordinator of Data and Statistics for review. If the request is approved, an MOA is drafted and sent to legal, placed on the board consent calendar, reviewed by the Superintendent, sent to the Purchasing/Contract Manager, sent to the Coordinator of Data and Statistics, appropriate Data Steward fulfills the request, de-identifies data as appropriate, and sends to another Data Steward for Quality Assurance (ensuring Student data protection). If it passes QA data is sent to the requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. If it does not pass QA the data is sent back to the Data Steward for modification.

DATA BREACH

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.

Policy:
THSA shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of PII, THSA staff shall follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, THSA shall follow best practices for notifying affect 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 member of the THSA executive team to determine whether a security breach has occurred. If the THSA data breach response team determines that one or more employees or contracted partners have substantially failed to comply with THSA's IT 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 involved IT Security Manager must be reported immediately to the Superintendent.
THSA will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach. THSA will make these resources available on its website.

Data Breach Response and Notification

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 outlined in the Agency IT Security Policy for responding to the breach.

Concerns about data breaches must be reported immediately to the IT security manager who will collaborate with appropriate members of the administration to determine whether a security

breach has occurred. If the LEA determines that one or more employees or contracted partners have substantially failed to comply with The LEA's 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 Superintendent.

Notification

The LEA 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.

The LEA shall always notify the parent or the adult student in the case of a significant data breach, as defined by Board Rule.

The LEA shall notify USBE of any data breach from a third party.

Record Retention and Expungement

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.
Scope:
THSPA board members and staff.
Policy:
The THSA staff, Utah LEAs and schools 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.
In accordance with 53A-1-1407, THSPA shall expunge student data that is stored upon request of the student if the student is at least 23 years old or as necessary. THSA may expunge medical records and behavioral test assessments. THSA will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information unless necessary. THSA staff will collaborate with Utah State Archives and Records Services in updating data retention schedules.

Retention

Records retention and expungement policies promote efficient management of records, preservation of records of enduring value, quality access to public information, and data privacy. LEA staff shall retain and dispose of student records in accordance with GRAMA, UCA 63G-2-604, and the Student Data Protection Act, 53E-9-306, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

Expungement

Expungement Request Policy

Tuacahn High School (THSA) recognizes the risk associated with data following a student year after year that could be used to mistreat the student. THSA 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. THSA shall decide whether to expunge the data within a reasonable time after the request.
3. If THSA decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
4. THSA shall hold the hearing within a reasonable time after receiving the request for a hearing.
5. THSA 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. THSA 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. THSA 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, THSA will seal it or make it otherwise unavailable to other staff and educators.

Data Transparency

Annually THSA will publically post:

THSA data collections
Metadata Dictionary as described in Utah's Student Data Protection Act

APPENDIX – **THSA Employee Non-Disclosure Agreement**

As an employee of THSA, I hereby afform that: (please initial)

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

_____I will abide by the terms of the THSA policies and its subordinate process and procedures.

_____I grant permission for the manual and electronic collection of retention of security related information, including but not limited to photographic or videotape images, or your attempts to access the facility and/or workstations.

Trainings

_____I have completed THSA Data Security and Privacy Fundamentals Training

_____I will complete THSA Data Security and Privacy Fundamentals Training within 30 days.

Using THSA's 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 computers or THSPA's system user accounts, with THSA staff or participating program staff.

_____I will log out of and close the browser after each use of THSA's data and reporting system.

_____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 PII in a locked location while unattended.

_____I will not share student/staff identifying data during 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 THSA server.

Reporting & Data Sharing

_____I will not re-disclose or share any confidential data analysis except to other authorized personnel with THSA's express written consent.

_____I will not publically publish any data except with the approval of the Superintendent.

_____I will take steps to avoid disclose of PII in state-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

_____I will not use e-mail to send screenshots, text, or attachments that contain PII 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 in writing.

_____I understand that when sharing student/staff-identifying data with authorized individuals the only approved methods are phone calls or THSA's secure file transfer protocol. Also, sharing within secured servers folders is appropriate for THSA 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 THSA IT officer. 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 THSA 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 THSA I will not disclose or otherwise disseminate any confidential or PII to anyone outside of THSA without prior written permission of the Student Data Manager of THSA.

Print Name:_____ Date:_____

Signature:_____