6303 Data Governance Plan

1 SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, volunteers and contractors of the Agency. The policy must be used to assess agreements made to disclose data to third-parties. This policy is designed to ensure only authorized disclosure of confidential information.

Furthermore, this *Pioneer High School for the Performing Arts* (hereafter, PHS) Data Governance Plan works in conjunction with the PHS Technology Security Policy Individual and Group Responsibilities

The following tables outlines individual *PHS* staff and advisory group responsibilities.

Role	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 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 student 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 LEA staff that have access to personally identifiable student data. 6. Ensure annual LEA level 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 *PHS* employees; and 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 *PHS*' systems security needs
Goverance Commitee	1. Review state law and rule regularly to ensure data security policies are in compliance.
Staff	1. Receive annual data privacy training. 2. Sign annual non-disclosure assurances 3. Protect logins, passwords, and all student data as directed in training.

2 EMPLOYEE NON-DISCLOSURE ASSURANCES

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

2.1 SCOPE

All *PHS* board members, employees, contractors and volunteers must sign and obey the *PHS* Employee Non-Disclosure Agreement, which describes the permissible uses of state technology and information.

2.2 NON-COMPLIANCE

Non-compliance with the agreements may result in consequences outlined in 3113 Volunteer Service and 6304 Disciplinary Action Non-Disclosure Assurances

All student data utilized by *PHS* is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way *PHS* staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all *PHS* staff to verify agreement to adhere to/abide by these practices. All *PHS* 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 *PHS' Student Data Manager* 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 when disposing of such records.
9. NOT share personally identifying data during public presentations, webinars, personal discussions not necessary for job duties, 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 Privacy Manager should be consulted..
14. Use secure methods when sharing or transmitting sensitive data. Also, sharing within secured server folders is appropriate for *PHS* 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 in item ten.
16. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

2.3 DATA SECURITY AND PRIVACY TRAINING

2.3.1 Purpose

PHS will provide a range of 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.

2.3.2 Scope

All *PHS* board members, employees, and contracted partners.

2.3.3 Compliance

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

2.3.4 Policy

1. Within the first week of employment, all board members, employees, and contracted partners must sign and follow the Employee Acceptable Use Policy and the Non-Disclosure Agreement, which describes the permissible uses of state technology, information, and data.
2. All current 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.
3. 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 board members, employees, and contracted partners who do not have these requirements completed to the IT Security Manager.

3 DATA DISCLOSURE

3.1 PURPOSE

Providing data to persons and entities outside of PHS 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 *PHS*. 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.

3.2 POLICY FOR DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

3.2.1 Student or Student's Parent/Guardian Access

Parents are advised that the records maintained by *PHS* are provided to *PHS* by the school in which their student is/was enrolled, and 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. LEAs are not required to provide data that it does not maintain, nor is *PHS* required to create education records in response to an eligible student's request.

3.2.2 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 *PHS* 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 *PHS* without third-party verification that they are compliant with federal and state law, and board rule.

3.2.3 Governmental Agency Requests

PHS 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 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 that the request is in accordance with state and federal law.

3.3 Data Disclosure to a Requesting External Researcher or Evaluator

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

PHS 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 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. A *PHS* Director, Superintendent, or board member sponsors an external researcher or evaluator request.
2. Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Coordinator of Data and Statistics.
3. Researchers and evaluators supply the *PHS* a copy of any publication or presentation that uses *PHS* 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 Coordinator or Data and Statistics, appropriate Data Steward fulfills request, de-identifies data as appropriate, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.

4 DATA BREACH

4.1 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.

4.2 POLICY

PHS shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, staff shall follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, *PHS* 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 executive committee to determine whether a security breach has occurred. If the data breach response team determines that one or more employees or contracted partners have substantially failed to comply with Technology Security Policy and relevant privacy policies, they will identify appropriate consequences in accordance with 3113 Volunteer Service or 6304 Disciplinary Policy. Concerns about security breaches that involve the IT Security Manager must be reported immediately to the School Leader.

PHS will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach. *PHS* will make these resources available on its website.

Record retention and expungement

4.3 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.

4.4 SCOPE

PHS board members and staff.

4.5 POLICY

PHS 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, PHS shall expunge student data that is stored upon request of the student if the student is at least 23 years old. PHS may expunge medical records and behavioral test assessments. *PHS* will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. *PHS* staff will collaborate with Utah State Achieves and Records Services in updating data retention schedules.

PHS maintained student-level discipline data will be expunged after three years.

5 QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS

5.1 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:

5.1.1 Data Governance Structure

The data governance policy is structured to encourage the effective and appropriate use of educational data. The data governance structure centers on the idea that data is the responsibility of all *stakeholders* 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.

5.1.2 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 (USBE)* communicates data requirements and definitions to PHS through the Data Clearinghouse Update Transactions documentation (see http://www.schools.utah.gov/computerservices/Data-Clearinghouse.aspx).

On the data reporting side, the production and presentation layers provide standard data definitions and business rules. 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.

5.1.3 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, *USBE* provides to PHS clear guidelines for data collection and the purpose of the data request. USBE also notifies PHS as soon as possible about future data collections. Time must be given to schools in order for them to begin gathering the data needed.

5.1.4 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 schools in explaining and/or correcting the anomalies. Data Analysts also work with School Finance to address findings from the Auditors.

5.1.5 Quality Control Checklist

Checklists have been proven to increase quality Therefore, before releasing high-risk data, Data Stewards and Data Analysts must successfully complete the data release checklist in three areas: reliability, validity and presentation.

6 DATA TRANSPARENCY

Annually, *PHS* will publicly post:

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

Board Approved: 10/18/2017