PACIFIC HERITAGE ACADEMY DATA GOVERNANCE PLAN

1. Purpose and Scope

1.1 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. Pacific Heritage Academy (referred to as "the LEA" throughout) 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. §53E, Chapter 9, Part 3, requires that the LEA adopt a Data Governance Plan.

1.2 Scope

This policy is applicable to all employees, temporary employees, and contractors of the LEA. 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 LEA 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 subsections provide data governance policies and processes to ensure compliance with federal and state law and board rule:

1. Purpose and Scope
2. Organization and Roles
3. Parent and Student Rights
4. Collection of Data
5. Maintenance and Protection of Data
6. Data Disclosures
7. Record Retention and Expungement
8. Data Breach Response and Notification
9. Technical Assistance, Training, and Support
10. Data Quality, Auditing, and Transparency

2. 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.

3. Parent and Student Rights

3.1 Definition of parent

A parent is defined as the biological parent, a legal guardian, or an individual in charge of the day-to-day care of the student. In cases where biological parents are separated or divorced, both parents shall have these rights unless there is a court order, State statute, or legally binding document that has revoked these rights to one or both of the parents.

3.2 Right to access

Per FERPA, parents of students who are minors (have not turned 18 yet) and adult students shall be given access to the student's data. In general, this access will be given via the LEA's student information system (SIS). Other requests will be granted within a reasonable period, but in no case greater than 45 days after the request was made.

3.3 Right to seek to amend

In 34 CFR 99, Subpart C, FERPA describes a parent's right to seek to amend any educational record they believe is inaccurate, misleading, or in violation of the student's right to privacy. The LEA shall then decide whether to amend the record within a reasonable amount of time.

If the LEA decides not to amend the record, the parent will be informed of their right to a hearing. The hearing will only be held at the parent's request, and the format of the hearing will be determined on a case-by-case basis.

Should the hearing determine that the record should not be amended, the LEA will inform the parent of the right to place a statement in the record commenting on the contested information. This statement will be maintained by the LEA and be included in any disclosures related to the record.

3.4 Right to consent to disclose

A parent may submit written consent to disclose information from a student's education record to any individual or entity. The requirements for these disclosures are found in Section of 6.1 of this plan.

4. Collection of Data

4.1 Prohibited collections

Per UCA 53E-9-305(2), the LEA will not collect a student's social security number or, except as required in UCA 78A-6-112(3), criminal record.

4.2 Collections only permitted with prior parental consent

4.2.1 Utah FERPA

Per UCA 53E-9-203, the LEA will prohibit the administration of any psychological or psychiatric examination, test, or treatment, or any survey, analysis, or evaluation that has the purpose or evident intended effect to have a student reveal any of the following personal information about themselves or concerning a family member's unless written parental consent is received:

- Political affiliations or, as provided by UCA 53G-10-202 or USBE Board Rule, political philosophies
- Mental or psychological problems
- Sexual behavior, orientation, or attitudes
- Illegal, anti-social, self-incriminating, or demeaning behavior
- Critical appraisals of individuals with whom the student or family member has close family relationships
- Religious affiliations or beliefs
- Legally recognized privileged and analogous relationships, such as those with lawyers, medical personnel, or ministers
- And income, except as required by law

Written parental consent will only be valid if a parent or legal guardian has been given two-week's prior notice, including a copy of the questions in the case of the survey, that includes

- Which records or information are to be examined
- The means by which they will be examined
- The means by which the information will be obtained
- The purpose for which the records or information are needed
- The entities or persons who will have access to the records
- The method by which a parent or student may access the records

If a school employee believes that collecting any of these information is necessary to respond to an emergency, then the employee may collect the information in accordance with the LEA's Incident Response Plan.

4.2.2 Optional data

In addition, the LEA shall annually designate all information not necessary for day-to-day school functions as "optional" data. Per 53E-9-301(16), optional student data includes information that is

- Related to an IEP or needed to provide special needs services
- Biometric information, which means a retina or iris scan, fingerprint, human biological sample, or scan of hand or face geometry
- Any data not designated as necessary student data

Optional data will only be collected with prior parental consent.

4.3 Parental notification

Per 53E-9-305(2), the LEA shall annually prepare and distribute to parents and students a collection notice statement that

- Is a prominent, stand-alone document
- Is annually updated and published on the LEA's website
- States the necessary and optional data that the LEA collects
- States that the LEA shall not collect of the prohibited data in Section 4.1
- States the data that the school may not share without written parental consent
- Includes the statement "The collection, use, and sharing of student data has both benefits and risks. Parents and students should learn about these benefits and risks and make choices regarding student data accordingly."
- Describes in general terms how the LEA will store and protect the data
- States a student's rights to the data
- Requests written consent for students in grades 9 – 12 to have their contact information shared with the state Board of Regents for the purpose of higher education outreach

Should the LEA choose, the collection notice statement and any collection of written consent to share optional information may be separate documents.

5. Maintenance and Protection of Data

5.1 Best practices

The LEA shall use reasonable data industry best practices to maintain and protect student data and other education-related data, including teacher and employee data.

Should the LEA contract with a third-party provider to collect, maintain, and have access to student data, the LEA shall ensure that the contract with the provider includes a provision that the data are the property of the student and that the data will not be redisclosed with the student's consent. The LEA will ultimately monitor and maintain control of the data.

All data will be maintained in accordance with the LEA Information Technology Systems Security Plan, as described in R277-487-2(11).

5.2 Employee expectations and assurances

Per Board Rule R277-487-3, all employees, aides, and volunteers of the LEA shall maintain appropriate confidentiality pursuant to federal, state, local laws, and this and other LEA policies with regard to student performance data and personally identifiable student information.

An employee, aide, or volunteer may not share, disclose, or disseminate passwords that are used to access student performance data or any personally identifiable student information per R277-487-3(17).

LEA employees may only access student records pursuant to a legitimate educational purpose and consistent with their educator obligations under R277-515.

All LEA employees that have access to confidential data shall receive an annual training regarding data governance and student data privacy requirements as described in Section 9.1. School employees shall annually submit a certified statement to the LEA data manager upon completion of this training.

The LEA may use a nondisclosure agreement (NDA) or other methods to ensure that all LEA employees meet these expectations. Licensed educators in violation of this NDA, this data governance plan, or Board Rule R277-487 may be subject to disciplinary action by the LEA or by the Utah State Board of Education.

6. 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.

6.1 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.

6.2 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. These can be found in more detail in Table 2.

6.2.1 External Research Review Process

All external research requests must be submitted to the LEA's external research review process to determine whether the research is for or on the LEA's behalf and whether it meets the requirements of FERPA found in 34 CFR 99.31(6). The LEA will then determine if the data may be shared with personally identifiable information, de-identified information, aggregated data, or not at all.

6.2.2 Third-party contractors

The LEA may contract services to third parties using the School Official exception in FERPA. When contracting with any third party, except for cases of general audience websites or where parental consent is obtained, the contract will specify the following:

- Requirements and restrictions related to the collection, use, storage, or sharing of student data by the contractor that are necessary for the education entity to ensure compliance
- A description of a person, or type of person, including an affiliate of the third-party contractor, with whom the third-party contractor may share student data
- Provisions that govern the deletion of the student data by the contractor
- Provisions that prohibit the redisclosure of the data
- A right-to-audit clause

6.3 Recordation

All data disclosures will be recorded on the student's record per FERPA's recordation requirements found in 34 CFR 99.32. All third parties that receive data will be entered into the LEA's Metadata Dictionary. A link to the Metadata Dictionary will be available on the LEA's website.

7. Record Retention and Expungement

7.1 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.

7.2 Expungement

Per 53E-9-306, the LEA shall follow Board Rule regarding the categorization, maintenance, and expungement of student disciplinary records, medical records, and behavioral test records. In order to ensure maximum student data privacy, the LEA shall also delete student data once administrative need

has ended and in accordance with active records retention schedules and USBE Board Rule regarding the timeline and process for a prior student to request that records be expunged.

7.2.1 Records that may not be expunged

Per 53E-9-306, the following records may not be expunged:

- Grades
- Transcripts
- A record of the student's enrollment
- Assessment information

8. Data Breach Response and Notification

8.1 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.

8.2 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.

9. Training, Technical Assistance, and Support

9.1 Training

The Student Data Manager shall ensure that all employees, staff, and volunteers receive an annual training on data security and data privacy per 53E-9-204. The Data Manager shall maintain a list of

employees who have completed the training and provide a certified statement, signed by the employees, that verifies their completion. Employees who have not received this training will not be given access to student data.

Furthermore, the LEA 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.

The LEA may arrange for the State Student Data Privacy Trainer to provide trainings or training materials.

9.2 Technical assistance and support

The Student Data Manager will provide technical assistance and support to educators, staff, employees, and volunteers as needed.

10. Data Quality, Auditing, and Transparency

10.1 Data quality

The Student Data Manager, IT Security Manager, and any other LEA employees as designated under the direction of the data governance group shall perform regular and ad hoc data auditing for quality assurance. Data sets and reports will be reviewed for reliability, validity, and presentation before they are disclosed.

10.2 Auditing and monitoring

10.2.1 Third party audits

As permitted by 53E-9-309(2), the LEA shall seek evidence of compliance, up to and including an audit by the LEA or a designee, to verify that all third parties contracted by the LEA are in compliance with Federal and State law, this data governance plan, and all terms of the contract.

10.2.2 LEA audits and evidence of compliance

The LEA shall annually provide to the State Superintendent evidence of compliance with Federal and State data confidentiality and disclosure laws to be reviewed by USBE's Chief Privacy Officer annually by October 1, per R277-487-3(13).

The LEA shall furthermore coordinate with the USBE Student Data Privacy Auditor regarding ad hoc audits of the LEA's compliance with Federal and State law and this data governance plan.

10.3 Transparency

The LEA shall annually publish the following on its website:

- This data governance plan
- A URL link to the LEA Metadata Dictionary

Table 1. Data governance roles and responsibilities

Role	Responsibilities
LEA Student Data Manager	1. Authorize and manage the sharing, outside of the education entity, of personally identifiable student data 2. Act as the primary local point of contact for the state student data officer. 3. Create and maintain a list of all LEA staff that have access to personally identifiable student data. 4. 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. Act as the primary point of contact for state student data security administration in assisting the board to administer this part; 2. Ensure compliance with security systems laws throughout the public education system, including: a. providing training and support to applicable LEA employees; and b. producing resource materials, model plans, and model forms for LEA systems security; 3. Investigate complaints of alleged violations of systems breaches

Table 2. FERPA exceptions

Exception	Who	Assurances	Redisclosure Restrictions
Accreditation	Accrediting Organization	Data may be shared as needed for the organization to carry out its accrediting functions	No redisclosures without parent or student permission or in response to a judicial order/subpoena
Audit/Evaluation	Individuals or agencies designated as "authorized representatives" of the LEA for the purpose of audit or evaluation of a federal or state education program	Written agreement that specifies • who the authorized representative is • the data to be shared • requirements to destroy the data once no longer needed • the time period to destroy the data • Policies and procedures to ensure confidentiality and privacy	No redisclosures without parent or student permission or in response to a judicial order/subpoena or if required by federal law
Caseworkers	Caseworkers of the Department of Human Services or Juvenile Justice Court	Caseworker must have a legal right to access the data, and the student must be under the care and protection of the caseworker per Utah law	The Student Data Protection Act allows redisclosures to other caseworkers in order to improve educational outcomes for youth
Child Nutrition Data	Department of Agriculture, or an authorized representative or contractor of the Food and Nutrition Service	The National School Lunch Program has higher restrictions on child nutrition program data	No redisclosures without parent or student permission or in response to a judicial order/subpoena
Dependent Student	Parents of students who have turned 18 but are still claimed as a dependent on the parent's taxes	Per LEA policy to determine the student is a dependent	None
Directory Information	Any party as designated in the LEA's annual directory information notice	LEA must annually notify parents of their directory information policy. Parents must be given a reasonable amount of time to opt out.	None

Financial Aid	Individuals or agencies who need the student information to determine the eligibility, amount, and conditions of financial aid OR to enforce the terms and conditions of financial aid	None	No redisclosures without parent or student permission or in response to a judicial order/subpoena
Health or Safety Emergency	Appropriate parties in connection with an emergency	LEA must determine that there is a clear and articulable threat	No redisclosures without parent or student permission or in response to a judicial order/subpoena
Juvenile Justice	An alternative school-related intervention run by the Department of Juvenile Justice Services per UCA 53G-8-211	Student must be "prior to adjudication"	No redisclosures without parent or student permission or in response to a judicial order/subpoena
School Official	Teachers and contractors, consultants, volunteers that perform a service or function for which the LEA would use its employees	Must be under direct control of the LEA, as defined by contract, NDA, physical or technical controls, or other agreement specified by the LEA	No redisclosures without parent or student permission or in response to a judicial order/subpoena
Sex Offenders	Individuals who need to know in connection to sex offenders or other individuals required to register under the Violent Crime Control and Law Enforcement Act	None	None
Student Transfer	Officials of another school that the student is attending or seeks to enroll	LEA must make a reasonable effort to notify the parent of the disclosure. This may be done in the LEA's annual FERPA notice.	No redisclosures without parent or student permission or in response to a judicial order/subpoena

Studies	Researchers working for or on the behalf of the LEA to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction	Written agreement that specifies • purpose, scope, and duration of the studies • that the data may only be used for the study • restrictions on personal identification of the data • a requirement to destroy the data at the end of the study	No redisclosures without parent or student permission or in response to a judicial order/subpoena
Subpoena/Judicial Order	Any judicial or legislative authority that issues a subpoena or judicial order	Parents must be notified of the subpoena/judicial order and given enough time to seek protective action	None per FERPA. Utah's Student Data Protection Act, however, restricts the redisclosure for any purposes outside the subpoena/judicial order