Student Data Governance Plan

Introduction

Purpose

The Park City School District (PCSD) affirms that the efficient collection, analysis, and storage of student information are essential to improve the education of our students. PCSD recognizes the need to exercise care in the handling of confidential student information as the use of student data has increased and as technology has advanced. PCSD also acknowledges that the privacy of students and the use of confidential student information is protected by federal and state laws, including the federal Family Educational Rights and Privacy Act (FERPA), the Utah Family Educational Rights and Privacy Act, and the Utah Student Data Protection Act.

This Data Governance Plan (Plan) is adopted pursuant to the Utah Student Data Protection Act and is intended to provide guidance regarding the collection, access, security and use of education data to protect student privacy. It is consistent with the Utah Student Data Protection Act regarding the access, security, and use of data maintained within the District and its individual schools. PCSD has established processes for managing student data collection and use to comply with state law.

Scope and Applicability

This Plan is applicable to all board members, employees, temporary employees, volunteers, and contractors of PCSD. The Plan must be used to assess agreements made to disclose data to third-parties. This Plan must also be used to assess the risk of conducting business. In accordance with PCSD policy and procedures, this Plan will be reviewed on an annual basis or more frequently, as needed. This policy is designed to ensure only authorized disclosure of confidential information.

Non-Compliance

Non-compliance with the requirements of this Plan may result in loss of access to Student Data or PCSD network on which it is maintained. Employees and contractors may be subject to disciplinary action, up to and including termination of employment, and termination of any agreement under which contract work is performed.

Definitions

Administrative Security consists of policies, procedures, and personnel controls including security policies, training, audits, technical training, supervision, separation of duties, rotation of duties, recruiting and termination procedures, user access control, background checks,

performance evaluations, disaster recovery, contingency, and emergency plans. These measures ensure that authorized users know and understand how to properly use the system in order to maintain security of data.

Aggregate Data is collected or reported at a group, cohort, or institutional level and does not contain Personally Identifiable Student Data (PISD).

Data Breach is the unauthorized release or acquisition of a student's PISD.

Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights, and authority levels. These measures ensure that only authorized users are able to perform actions or access information in a network or a workstation.

Personally Identifiable Student Data (PISD) includes: a student's name; the name of the student's family; the student's address; the student's social security number; a student education unique identification number or biometric record; or other indirect identifiers such as a student's date of birth, place of birth, or mother's maiden name; and other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community who does not have personal knowledge of the relevant circumstances to identify the student.

Physical Security describes security measures designed to deny unauthorized access to facilities or equipment.

Student Data means data collected at the student level and included in a student's educational records. Student data may or may not be Personally Identifiable Student Data, but does not include aggregate or de-identified data.

Unauthorized Data Disclosure is the intentional or unintentional release of PISD to an unauthorized person or untrusted environment.

Roles and Responsibilities

The LEA acknowledges the need to identify parties who are ultimately responsible and accountable for data and content assets. These individuals and their responsibilities are as follows:

Student Data Manager

The Student Data Manager has the following duties:

- Authorize and manage the sharing, outside of the student data manager's education entity, of personally identifiable student data for the education entity as described in this section
- Provide for necessary technical assistance, training, and support
- Act as the primary local point of contact for the state student data officer
- Ensure that the following notices are available to parents:
    a. annual FERPA notice (see 34 CFR 99.7),
    b. directory information policy (see 34 CFR 99.37),
    c. survey policy and notice (see 20 USC 1232h and 53E-9-203),
    d. data collection notice (see 53E-9-305)

The Student Data Manager for PCSD will be Andrew Frink, Chief Information Officer.

Information Security Officer

- Oversee adoption of the CIS controls
- Provide for necessary technical assistance, training, and support as it relates to IT security

The Information Security Officer will be Joe Stout, Director of Technology Services

Public Posting of Policy and Procedure

Annually, PCSD will publicly post the following on the District website:

- Data Governance Plan (this document)
- Metadata Dictionary
- Student Data Disclosure Statement

Data Security

Data Security

PCSD has in place Administrative Security, Physical Security, and Logical Security controls to protect against a data breach or an unauthorized data disclosure.

Data Security and Privacy Training

PCSD will provide a range of training opportunities for all PCSD staff, including volunteers, contractors and temporary employees with access to student educational data in order to minimize the risk of human error and misuse of information.

1. All PCSD board members, employees, and volunteers with access to Student Data must sign and follow the PCSD Employee Acceptable Use Policy, which describes the permissible uses of PCSD technology and information.
2. All current PCSD board members, employees, and volunteers with access to Student Data are required to participate in an annual Security and Privacy Training.
3. PCSD requires a targeted Security and Privacy Training for other specific groups within the District that collect, store, or disclose Student Data. The Student Data Manager will identify these groups and will determine the annual training topics for these targeted groups based on PCSD training needs.
4. Participation in the training will be annually monitored by supervisors. Supervisors and the board secretary will annually report all PCSD board members, employees, and contracted partners who do not have these requirements completed to the Student Data Manager.

Data Breach

In the event of a data breach or other inadvertent release of PISD, PCSD staff shall follow industry best practices for responding to the breach, and shall comply with all notification requirements imposed by law, including:

- If the student is an adult, the student shall be notified of the release;
- If the student is a minor, the student's parent or legal guardian shall be notified;
- PCSD shall immediately notify the Utah State Board of Education (USBE) in the case of a confirmed data breach or a confirmed unauthorized data disclosure.

Concerns about data breaches must be reported immediately to the Student Data Manager who will collaborate with appropriate staff members to determine whether a data breach has occurred. If the PCSD data breach response team determines that one or more employees or contracted partners have substantially failed to comply with the PCSD policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action.

Auditing and Review

The Student Data Manager will conduct an annual audit and review of existing data access, policy, and security safeguards.

Data Disclosure

Personally Identifiable Student Data (PISD)

Student or Student's Parent/Guardian

A student owns the student's personally identifiable student data. PCSD will provide parents or legal guardians with access to their child's student data, or an adult student access to his or her own student data (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.

PCSD is not required to provide data that it does not maintain, nor is PCSD required to create Student Data in response to an eligible student's request.

School Officials

School officials will have access to PISD if the school official is determined to have a legitimate educational interest in that information. Examples of school officials include, but are not limited to, classroom teachers, school principals, school secretaries, school nurses, District administrators, technology staff, and cafeteria personnel.

Directory Information

PCSD can disclose directory information as defined and allowed under the federal Family Educational Rights and Privacy Act (FERPA), the Utah Family Educational Rights and Privacy Act, and PCSD policy District Family Educational Rights and Privacy Policy 11000.

Third Party Vendors

Third party vendors may have access to students' personally identifiable information if the vendor is designated by PCSD 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 vendors such as: nurses, counselors, attorneys, hearing officers and disciplinary boards, consultants, volunteers or other parties to whom the school has outsourced institutional services or functions.

All third-party vendors contracting with PCSD must be compliant with Utah's Student Data Protection Act, including, but not limited to Section 53A-1-1410. Vendors determined not to be compliant may not be allowed to enter into future contracts with PCSD without third-party verification that they are compliant with federal and state law.

Governmental Agency Requests

The Student Data Manager can disclose PISD under the following circumstances:

- to an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court;
- in response to a lawfully issued subpoena and/or court order, after complying with applicable requirements under FERPA;
- As otherwise allowed by law, such as with a valid parent consent.

In the case of a federal or state government agency request for PISD, the requesting governmental agency must provide evidence of the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions to data without consent, such as

- reporting requirement
- audit
- evaluation

The Student Data Manager will ensure the proper data disclosure protections 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."

Non-Personally Identifiable Student Data

External data requests from individuals or organizations that do not intend to conduct external research or are not fulfilling a state or federal reporting requirement, audit, or evaluation should be made to the Student Data Manager. The requests will be reviewed by the PCSD Administrative Cabinet and the District Statistician.

External Research or Evaluation

The Student Data Manager will ensure the proper data are shared with external researcher or evaluator to comply with federal, state, and board rules. PCSD may not disclose PISD to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program audit or evaluation,except as explicitly permitted by parent/guardian consent. Data that do not disclose PISD may be shared with external researcher or evaluators for projects unrelated to federal or state requirements if:

1. A PCSD Director, Superintendent, or board member sponsors an external researcher or evaluator request.

2. Student Data are not PISD and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the District Statistician.
3. Researchers and evaluators supply PCSD with a copy of any publication or presentation that uses PCSD data 10 business days prior to any publication or presentation.

Requests will be made to the Student Data Manager and will be reviewed by the PCSD Administrative Cabinet and the District Statistician.

Record Retention and Expungement

PCSD shall retain and dispose of student records in accordance with Section 63G-2-604 of the Utah Government Records Access and Management Act, Section 53A-1-1407 of the Student Data Protection Act, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

The LEA recognizes the risk associated with data following a student year after year that could be used to mistreat the student. The LEA shall review all requests for records expungement from parents and make a determination based on the following procedure.

Procedure for Requesting Expungement

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. The LEA shall decide whether to expunge the data within a reasonable time after the request.
3. If the LEA decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
4. The LEA shall hold the hearing within a reasonable time after receiving the request for a hearing.
5. The LEA 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. The LEA 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. The LEA 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, the LEA will seal it or make it otherwise unavailable to other staff and educators.

Related Documents

- Student Data Protection Act, Utah Code Ann. §§ 53A-1-1401 et seq.
- Utah Family Educational Rights and Privacy Act, Utah Code Ann. §§ 53A-13-301 et seq.
- District Acceptable Use Policy 9110
- District Family Educational Rights and Privacy Policy 11000
- District Records Management Policy 4020
- District Student Data Disclosure Statement