# 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 and PCSD policy and procedure for responding to the breach, and shall comply with all notification requirements imposed by law, including:

- In the event of a significant data breach, the LEA will notify (a) the student, or (b) the student's parent if the student is not an adult student, as required in R277-487-3(3)
- In the event of a significant data breach, the LEA will report the breach to the Utah State School Board within 10 business days of the initial discovery as required in R277-487-3(3)

## Initial Notification

When an employee suspects a breach has occurred or is made aware of a data breach of any kind, they must:

1. Put in a ticket in the Helpdesk system, under the "Network" category
    a. Include all known details of the incident, including any contact information for impacted vendors or copies of emails received
2. Call the IT department immediately. If no one is available, please leave a voicemail with the basic details of the incident (we will be able to look up the ticket for all of the details).
    a. Andrew Frink
    b. Joe Stout

## Response

Once the IT department personnel are aware of the incident, they will:

1. IT leadership will contact the Superintendent and Business Administrator and inform them of the issue and will create the incident leadership team
    a. The incident leadership team will include the Superintendent, Business Administrator, Communications, Chief Information Officer, Legal Counsel, and any other specifically related IT personnel as needed.
2. IT staff will investigate the incident to determine the scope and data involved
    a. Key information
        i. Data involved, list of impacted people, timeline
    b. If the breach was at a vendor, we will contact them directly for more information
    c. If the breach was from a district employee, we will contact the employee
3. Once the incident has been investigated, the following steps will be taken
    a. The PCSD Board of Education will be notified as appropriate
    b. The Utah Cyber Center and the Office of the Attorney General will be notified as required under 63A-19-405
    c. If appropriate the Chief Information Officer will contact the district's data breach insurance provider
    d. If student data (PII) has been released, the team will create a communications plan to notify the impacted students and their parents
    e. If employee data has been released, the team will create a communications plan to notify the impacted employees and create an action plan to minimize the impact on the employees.
4. If the breach was at a vendor
    a. The district will review the contract for any legal remedies
    b. The district will evaluate our continued relationship with the vendor
5. If the breach was internal
    a. An internal investigation will be undertaken to discover the reasons (technical or human)
    b. A plan will be put in place to remediate any issues discovered

## 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 53E-9-309. 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

Research can be an important tool to ensure our school system is equitable and empowers each student and their family. The Park City School District (PCSD) supports the conduct of educational research and strives to achieve this by collaborating with educators, students, families, community based organizations, and university partners –listening to and uplifting the stories of our communities.

As such, our district partners with school leaders, educators, students, families and the community to support novel research that contributes to organizational learning, planning and decision-making aligned to our district strategic goals and objectives. Additionally, we support grant-funding efforts that provide innovative research-practice partnerships with external

researchers and organizations on projects that include research and strategic planning, providing consultation and evaluation using academic data analysis, surveys, interviews and other quantitative, qualitative, and design-based research methods and communication. Priority projects seek to primarily support Teaching and Learning –early literacy, math, college and career readiness, school climate and continuous improvement. We view such collaborations as primary vehicles for change, grounding our work in district wide initiatives and accountability structures that are centered around the PCSD vision of being student centered with a focus and emphasis on the whole-child - our students are safe, supported, engaged, challenged, and healthy.

## Process

PCSD has implemented a rigorous research review process managed by the department of Teaching and Learning. Our district requires this process for all individuals and organizations interested in conducting human subjects or secondary administrative data research with Park City School District students and staff (note that staff includes school administrators, school leaders, and teachers). Our Teaching and Learning Department manages the formal review process for all internal and external research requests, evaluating proposals to ensure they are relevant to district strategic priorities, rigorous in methodological approach, and low risk and low burden for school leadership, educators, and study participants. Federal and state agencies, institutes of higher education, and individuals seeking to conduct research in Park City School District must have their research approved by the Park City School District Teaching and Learning Team. Complete and submit this Application to Conduct Research Form to have your research proposal reviewed.

Research projects approved should adhere to the following guiding principles:

- Equity guides all research at all stages.
- Projects produce knowledge that will inform district leaders as they make decisions about how to best support students.
- Impactful research projects are developed in partnership and collaboration with PCSD stakeholders, practitioners, and content experts.
- Project timelines are succinct and respect the urgency of potential high-impact decisions that need to be made.

## PCSD Research Review Committee

The PCSD Research Review Committee reviews applications for educational studies. The committee consists of representatives from the Departments of Data & Assessment, Student Services, Teaching & Learning, Health Services, Special Education, Educational Equity, Educational Technology, and other relevant district personnel depending on the scope of research represented in the proposed research.

The review committee generally meets 4 times per year on pre-scheduled dates and screens applications for:

- Relevance to districtwide strategic initiatives and goals
- Rigor of research methodology
- Risks/benefits to schools and study participants
- Burden to the district, schools, and study participants

**Committee members will recommend District participation in projects which:**
**(a)** have a sound experimental design and have all required materials; **(b)** will benefit education in the District; **(c)** will not unreasonably disrupt instructional or administrative time, nor violate other law or policy; **(d)** will not intrude on the privacy of District patrons or personnel; **(e)** agree to provide the District with the results of the research and allow the District to publish the results in whole or in part on publicly accessible platform(s), **(f)** will allow the District to obtain feedback from research participants concerning their satisfaction with their participation or their experiences in the research.

**PCSD will not approve applications which seek to:**
**(a)** study domains extraneous to the improvement of quality teaching and student learning; **(b)** conduct market research which doesn't correlate with the long-range objectives of the Board of Education; **(c)** conduct longitudinal research which requires tracking student placement and data from year to year; **(d)** recruit students and/or employees for research unrelated to district priorities, interests, or programs. **(e)** are of a financial benefit to parties or individuals in the district or community and are otherwise partisan unless those disclosures are made appropriately and the committee is in unanimous agreement.

**Research Application Review Process:**
Completed applications are first reviewed by the District Statistician/Data Analyst to ensure the application is complete, that the proposed research is appropriate, and that it is built upon a sound research design, methodology, and instrumentation. If the research meets these conditions the review process will follow one of two paths:

**a) First Path.** If the research is being conducted solely by a Park City School District teacher, specialist, or administrator, is simple in design and scope (e.g., Capstone project), is limited to the teachers classroom, and the researcher has their principal's or supervisor's approval, the research may be approved directly by the Research Review Committee. However, if the committee has concerns with the research or feels that additional perspectives are necessary, the research application will follow the 'Second Path.'
**b) Second Path.** If the research is complex in design and/or scope, or involves multiple teachers, classrooms, or schools, or is being conducted by any person(s) not affiliated with Park City School District, the Research Review Committee may bring on additional committee members from the departments with whom the research most closely aligns. Together with their specialists, the Research Review Committee will provide their recommendations for the proposed research to the Superintendent of the District.

Applicants will receive email notification of the committee's decision along with any conditions or recommendations. Research requests are reviewed as they come in during regularly pre-scheduled meetings of the District Teaching and Learning Department (see below for list of this year's scheduled meetings). Research request applications received between July 1st and September 1st will generally not be reviewed until at least mid-September. The review process is normally completed within 1-2 weeks of the next scheduled meeting if it follows the first path or up to 4 weeks if it follows the second path beginning when the research application is first received.

*PLEASE NOTE: District approval informs our school leadership and potential participants that your research methodology and research design have scientific merit, and that the focus of your research supports district research interests. However, district approval neither requires nor implies participation of PCSD staff, employees, students, or stakeholders in your research. Rather, upon district approval and prior to conducting your research, you must obtain the active written consent of the principal from whose school you are seeking or recruiting participants as well as the written active consent of all potential participants and their legal guardians.*

## Data Collection

**Primary Data Collection: Students**

- Active consent continues to be required in order to collect primary data from students, as per the PCSD Policy; remote consent can be obtained so long as the information is securely stored.
    - PCSD may conduct an audit of electronic consents forms for any reason and at any time in order to validate the collected information.
- Remote one-to-one research activities involving students (i.e., interviews) are prohibited, per the Student Acceptable Use Policy.
- The researcher must secure a PCSD staff volunteer for any virtual focus group involving students. The selected CPS staff member (identified by the PCSD Central Office project lead) must (1) host the virtual meeting and (2) remain in attendance for the full duration of the focus group.
- Background checks will be required as per usual; researchers will need Level 1 background checks. Returning researchers may not need to reapply, but new researchers will need to go through the background check process.
- If approved, all virtual focus groups or interviews with students must be conducted through the PCSD -verified conferencing platform, Google Meets.

**Primary Data Collection: Staff**

- Principals must agree that the research is of value in their community, and that their staff has capacity to participate in the research.
- The burden on schools of recruiting research participants must be minimal.

- We recommend, but do not require, that researchers utilize Google Meets for primary data collection from CPS staff.
- Active consent continues to be required; consent can be obtained remotely.

**Primary Data Collection: Parents/Families**

- Principals must agree that the research is of value in their community, and that their families have capacity to participate in the research.
- The burden on schools of recruiting research participants must be minimal.
- Active consent continues to be required; consent can be obtained remotely.

# 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 53E-9-306 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. §§ 53E-9-301 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
- Application to Conduct Research Form