# PROVO CITY SCHOOL DISTRICT DATA GOVERNANCE PLAN

## PURPOSE OF PCSD DATA GOVERNANCE PLAN

The purpose of this Data Governance Plan is to meet the requirements of Utah's Student Data Protection Act ("SDPA"), UTAH CODE ANN. § 53E-9-301. SDPA requires the creation, maintenance, and publication of said plan. Provo City School District (PCSD) takes seriously its moral and legal responsibility to protect student privacy and ensure data security. The plan will encompass the full life-cycle of student data- beginning with acquisition, to use, to disposal of acquired data.

## SCOPE AND APPLICABILITY OF PCSD DATA GOVERNANCE PLAN

The PCSD Data Governance Plan is applicable to all PCSD employees, whether full or part-time, temporary employees, volunteers, and affiliated vendors and/or third-party contractors that collect, use, and/or share student data. This plan will be reviewed annually, at minimum, with necessary adjustments being made as required to meet the data privacy and security standards of PCSD and in accordance with state and/or federal law. This plan is designed to ensure that data is collected, used, and disposed of according to applicable federal and state law governing data privacy and security, and to ensure only authorized disclosure of confidential information. The plan outlines the following subsections and provides for data governance policies and process for Provo City School District:

1. Data Privacy Organizational Structure
2. Definitions Related to Data Privacy
3. Information Technology System Security Plan
4. Training, Technical Assistance, and Auditing
5. Student Data Collection, Use, and Disclosure
6. Employee Non-disclosure Assurance
7. Change of Employment or Separation From PCSD
8. Data Retention and Expungement
9. Data Incident/Breach Response Plan

In accordance with district guidelines, this plan will be reviewed and adjusted on at least an annual basis. This plan is designed to accomplish the following statutory requirements:

To incorporates reasonable data-industry best practices to maintain and protect student data and other education-related data

a. To provide for necessary technical assistance, training, support, and auditing
b. To describe the process for collecting, using, and sharing student data between an educational entity and another person
c. To describe the process for an adult student or parent to request that data be expunged from a student record.

**DEFINITIONS RELATED TO DATA PRIVACY**

**Access**: To directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

**Authorization**: The express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

**Computer**: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.

**Computer system**: A set of related, connected or unconnected, devices, software, or other related computer equipment.

**Computer network**: The interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals. **Computer property**: Electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, or any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them. **Confidential**: when applied to data, text, or computer property, means protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

**Encryption**: altered or converted into a cipher or code to conceal data in a way that requires a secret key or password to be decrypted or converted back to an original readable format. **Personally Identifiable Information (PII):** data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

**Security system**: a computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons. **System level access**: access to the system that is considered full administrative access and includes operating system access and hosted application access.

## Cybersecurity CIS 18 Plan

"In accordance with R277-487, Provo City School District has chosen to adopt the Center for Internet Security® Critical Security Controls framework; https://www.cisecurity.org/controls. Provo City School District will implement safeguards as recommended by the framework based on current implementations and risk assessments. These risk assessments will estimate the likelihood that an event will create an impact and these safeguards will help mitigate those risks. As the CIS Controls receives updates, Provo City School District will adjust plans and implementations accordingly. Provo City School District will also report to the USBE by October 1 each year regarding the status of the adoption of the framework and future plans for improvement."

- Consistent with the SDPA, this plan “incorporates reasonable data industry best practices to maintain and protect student data and other education-related data.” UTAH CODE ANN. § 53E-9-301(6). Such practices are set forth in **PCSD’s Policy sections 4202 and 4204** required by UTAH ADMIN. CODE r277-487-3(14). **As required by law, this CIS 18 plan will be implemented across the district. For questions, please contact the PCSD Tech Department.**

- Third party providers will be required to sign a contractual agreement guaranteeing the use of business best practices for the protection of student data including the immediate destruction of data upon termination of contract.

**TRAINING, TECHNICAL ASSISTANCE, AND AUDITING**

- Consistent with SDPA, this plan "provides for necessary technical assistance, training, support, and auditing." UTAH CODE ANN. § 53E-9-301(6).
- PCSD will provide training on FERPA, SDPA, district policies and guidelines related to computer use, records management, and student records. All employees, volunteers, and independent contractors who have access to student PII must complete the training before using District networks or electronic devices. The training may be incorporated into the PCSD's annual **Safe Schools** training.
- Participation in the training will be monitored and recorded by supervisors.
- All employees and independent contractors must sign the **Computer Use Agreement**, which describes the permissible uses of PCSD technology and information. Electronic signatures or other verification of agreement by employees after logging in to the Employee Portal constitute signature of the agreement.

## Data Privacy Organizational Structure

| Role | Responsibilities |
|---|---|
| **Data Privacy Coordinator** | 1. To act as point of contact for all Provo City School District personnel who use and/or receive student data in any capacity<br>2. To ensure compliance with all student data privacy laws within the public education system, to include:<br>a. Providing yearly data privacy training and support as required per applicable student data privacy laws<br>b. Investigating complaints and alleged violations of the Student Data Protection Act and/or FEREPA<br>c. Reporting violations and/or complaints to: local LEA board; applicable educational entities and/or personnel; the data privacy committee<br>d. Coordinating data transfers between Elementary and Middle Schools; Middle Schools and High Schools<br>e. Acting as the Provo City School District Data Manager |

| | |
|---|---|
| **Information Technology Systems Officers** | 1. To act as primary point of contact for Provo City School District IT Security personnel<br>2. Apply applicable laws and requirements to the IT Security System used within the Provo City School District by:<br>a. Providing training and support to applicable PCSD employees<br>b. Producing resources, materials, model plans and forms for PCSD system security that align with CIS standards<br>c. Investigating complaints of incidents and breaches that occur within the IT Security system, and reporting such incidences and breaches to applicable PCSD personnel and the Data Privacy Committee<br>d. Putting in place an incident and/or breach protocol to be followed if such instances<br>3. Providing a yearly report to the PCSD School Board and Superintendent of PCSD Security System needs |
| **Data Stewards** | 1. To act as point of contact for data related issues in each department and/or section of the PCSD to include:<br>a. Schools, district office, school board, E-school, etc.<br>2. Coordinates data projects with Data Privacy Coordinator and IT personnel as applicable to include: expungement procedures and timelines, archiving procedures, data transfers, etc.<br>3. Maintains a data record of all data collected, the reason for its use,and how/when the data will be destroyed/archived |

## STUDENT DATA COLLECTION, USE, AND DISCLOSURE

- Consistent with SDPA, PCSD's Superintendent will "designate an individual to act as the student data manager." UTAH CODE ANN. § 53E-9-303(2). Consistent with USBE rule, the Data Privacy Coordinator "authorizes and manages the sharing of student data; acts as the primary contact for the State Chief Privacy Officer; maintains a list of persons with access to personally identifiable student information; and is in charge of providing annual PCSD training on data privacy." UTAH ADMIN. CODE R277-487-2(19). This plan "describes the process for sharing student data between PCSD and another person or entity." UTAH CODE ANN. § 53E-9-301(6)(c). Student PII may be shared only in accordance with FERPA and PCSD guidelines set forth by this plan.

## ACCESS BY PARENTS

- Parents generally have a right to inspect and review the education records of their children. Access to the education records of a student who is or has been in attendance at a school in PCSD shall be granted to the parent of the student who is a minor or who is a dependent for tax purposes. The school shall presume that each parent, regardless of custody designation, has authority to inspect and review their student's records unless the school has been provided a copy of a court order, state statute, or other legally binding document that specifically revokes these rights.
- Parents may request an expungement of a record by making a written request to the Data Privacy Coordinator. All applicable laws, policies, and procedures will be followed concerning expungement of records. The Data Privacy Coordinator will determine if the request is valid and make the appropriate decision about the expungement. If the parent is not satisfied with the decision, they may request a hearing with the Director of Student Services, in writing, in order to explain their rationale for wanting the record expunged. A three person committee will meet to examine the request and make a determination, and render a decision. If the parent is still not satisfied, they may make a final appeal to the PCSD Superintendent, who will them render a final decision on the request to expunge the record in question.
- A parent's right to inspect and review his/her student's education record includes the right to access attendance records, test scores, grades, psychological records, applications for admission to other schools/colleges, and health or immunization information.
- If material in the education record of a student includes information on another student, only the portion of the material relating to the student whose records were requested may be inspected and reviewed.

## ACCESS BY STUDENTS

- Notwithstanding the rights afforded to parents, students in PCSD may also inspect and review their own educational record in accordance with processes set forth by the school that maintains the records.
- When a student reaches eighteen (18) years of age or is attending an institution of post-secondary education, the rights accorded to, and consent required of parents transfer from the parents to the student. If the student remains a dependent for tax purposes, the parents still have the right to access student records, until such time as the student is emancipated.

## ACCESS BY SCHOOL OFFICIALS

- School officials who have a legitimate educational interest in a student's education record may access the record without parental consent.
- For the purpose of this plan, "school officials" shall mean any employee, trustee, or agent of PCSD, or of facilities with which PCSD contracts for placement of students with disabilities. The term also includes attorneys, consultants, and independent contractors who are retained by PCSD, or by facilities with which PCSD contracts for placement of students with disabilities.
- School officials have a legitimate educational interest in a student's records when they are working with the student, considering disciplinary or academic actions, reviewing an individualized education plan (IEP) for a student with disabilities, compiling statistical data, or investigating or evaluating programs that may involve the student.

## ACCESS BY OTHER PERSONS

- PII in education records shall not be released, except to the following:
- 1. Individuals for whom the parent has given written consent. Parents should use PCSD Consent to Release Educational Records of Student Form

2. School officials, including teachers, who have legitimate educational interests
3. Officials of other schools, school systems, or institutions of postsecondary education in which the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer
4. Authorized representatives of the Comptroller General of the United States, the Secretary of Education, or state and local educational authorities who require access to student or other records necessary in connection with the audit and evaluation of federal or state supported education programs or in connection with the enforcement of or compliance with federal legal requirements that relate to such programs
5. Personnel involved with the student's application for, or receipt of, financial aid
6. Organizations conducting studies for educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction. Such studies must be conducted so that personally identifiable information (PII) of students and their parents will not be revealed to the entity doing the studies- only aggregate data may be provided to the entities doing said studies.
7. Accrediting organizations that require the information for purposes of accreditation
8. Parents of a student who is a dependent for tax purposes
9. The student
10. Individuals authorized by a judicial order or lawfully issued subpoena
11. Appropriate persons who, in an emergency, must have such information in order to protect the health or safety of the student or other persons
12. Persons or organizations authorized by the school's administration to obtain directory information
13. An agency caseworker or other representative of a state or local child welfare agency who provides documentation showing the right of that caseworker or representative to access the specific student's case plan. If shared with the Department of Human Services, the Department must be legally responsible for the care and protection of the student or providing services to the student. The student's PII may not be shared with a person who is not authorized to address the student's education needs. Consistent with UTAH CODE ANN. § 53E-9-308(4), a school official may share education information, including a student's personally identifiable student data, to improve education outcomes for youth:

A. In the custody of, or under the guardianship of, the Department of Human Services;
B. Receiving services from the Division of Juvenile Justice Services;
C. In the custody of the Division of Child and Family Services;
D. Receiving services from the Division of Services for People with Disabilities; or
E. Under the jurisdiction of the Utah Juvenile Court.

- The parent shall provide a signed and dated written consent before the school discloses personally identifiable information from a student's education records to any individual, agency, or organization other than the parent, the student, or those listed above. Such consent shall specify records to be released, the reason for such release, and to whom the

records are to be released. Parents should use PCSD Consent to Release Educational Records of Student form.

- Employees may not share student PII during presentations, webinars, or trainings. If an employee needs to demonstrate child/staff level data, demo records should be used rather than actual student PII.
- Employees must redact all student PII from any document that is shared with a general audience.
- Employees must take steps to avoid disclosure of student PII in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
- Consistent with UTAH CODE ANN. § 53E-9-303(4), PCSD has established the following process for a request for data for the purpose of external research or evaluation. Student PII may not be shared for the purpose of external research or evaluation.
- All student data requests for purposes of external research or evaluation must be submitted to the Director of Assessment, Data, and Research.
- The Director of Assessment, Data, and Research will ensure the proper data are shared with external researchers or evaluators to comply with federal, state, and board rules.
- Prior to conducting research or surveys in PCSD, approval must be obtained from Director of Assessment, Data, and Research.
- In order to conduct research or implement a survey, a Research Project Application must be completed and submitted to the Director of Assessment, Data, and Research
- Research Project Applications must be accompanied by a project proposal and must include a copy of the instruments that will be used.
- Research projects that require the participation of teachers and/or students during the first 30 days or the last 30 days of the school year will generally not be approved.
- Research proposal approval will generally be limited to those projects that complete the requirements associated with a graduate thesis, dissertation or practicum. A copy of the sponsoring college/university's approval letter and IRB letter must be attached to the application.
- Approval of the Research Project Application by the Curriculum Staff Committee authorizes the applicant to proceed with the research/survey. Committee approval does not obligate the participation of any school or employee.
- Following committee approval:
    1. No changes in methodology or instrumentation may be made unless approved by the Curriculum Staff Committee.
    2. A $100.00 refundable deposit is required. This deposit is to ensure that a copy of the research findings is shared with PCSD. Once a copy of the research results are received by the Director of Assessment, Data and Research, the $100.00 deposit will be refunded.
    3. Upon completion of the research project, a copy of the research findings is to be submitted to the Director of Assessment, Data, and Research.

## EMPLOYEE NON-DISCLOSURE ASSURANCE

- **SCOPE**: All PCSD board members, employees, contractors and volunteers must sign and adhere to the PCSD Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of state technology and information.

- **NON-COMPLIANCE** with the agreements shall result in consequences up to and including removal of access to PCSD network; if this access is required for employment, employees and contractors may be subject to dismissal.
- **NON-DISCLOSURE ASSURANCES**: All student data utilized by PCSD is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and SDPA. This plan outlines the manner in which PCSD staff are to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all PCSD staff to verify agreement to adhere to/abide by these practices and will be maintained in PCSD Human Resources office. All PCSD employees (including contract or temporary) will:
    - Complete a Security and Privacy Fundamentals Training.
    - Complete a Security and Privacy Training for Researchers and Evaluators, if your position is a research analyst or if requested by the Student Data Manager.
    - Consult with PCSD internal data owners when creating or disseminating reports containing data.
    - Use password-protected LEA-authorized computers when accessing any student-level or staff-level records.
    - Protect passwords.
    - **NOT** share individual passwords for personal computers or data systems with anyone.
    - **NOT** write down individual passwords for personal computers or data systems.
    - **NOT** auto-save individual passwords for auto-access to personal computers or data systems.
    - Log out of any data system/portal and close the browser after each use.
    - Store sensitive data on appropriate-secured locations. Unsecured access using 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.
    - Keep printed reports with personally identifiable information in a locked location while unattended and use the secure document destruction service provided at PCSD when disposing of such records.
    - **NOT** share personally identifying data during public presentations, webinars, etc. If users need to demonstrate student/staff level data, demo records should be used for such presentations.
    - Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the Data Privacy Coordinator, found in Appendix B (Protecting PII in Public Reporting).
    - Take steps to avoid disclosure of personally identifiable information (PII) in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
    - Delete files containing sensitive data after using them on computers or move them to secured servers or personal folders accessible only by authorized parties.
    - **NOT** use email to send screenshots, texts, 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 Coordinator should be consulted.

- Use secure methods when sharing or transmitting sensitive data. The approved method is PCSD's secure file transfer protocol (SFTP) website. Also, sharing within secured server folders is appropriate for PCSD internal file transfer.
- **NOT** transmit student/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods.
- Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

## CHANGE OF EMPLOYMENT OR SEPARATION FROM PCSD

1. As required, the Human Resource Department will contact all data managers immediately when employment responsibilities change due to separation from PCSD or change of assignment.
2. Upon notification of employment changes, PCSD will make immediate changes to access of student data, such as the removal or change of access from all data portals, dashboards, and reporting systems.

## DATA RETENTION AND EXPUNGEMENT

Utah LEAs and schools have the responsibility to retain and dispose of student records in accordance with section 63G-2-604, **53E-9-306**, and comply with active retention schedules for student records per Utah Division of Archive and Records Services.
In accordance with 53E-9-306, Parents may request an expungement of a record by making a written request to the Data Privacy Coordinator, in writing. All applicable laws, policies, and procedures will be followed concerning expungement of records. The Data Privacy Coordinator will determine if the request is valid and make the appropriate decision about the expungement. If the parent is not satisfied with the decision, they may request a hearing with the Director of Student Services, in writing, in order to explain their rationale for wanting the record expunged. A three-person committee will meet to examine the request and make a determination, and render a decision. If the parent is still not satisfied, they may make a final appeal to the PCSD Superintendent, who will then render a final decision on the request to expunge the record in question.

The LEAs /schools may expunge medical records, as well as behavioral test assessments. However, the LEA **shall not** expunge student records of grades, transcripts, student enrollment records, or assessment information. In accordance to Utah law, an LEA or school may create and maintain a cumulative disciplinary record for a student.

### Expungement Classifications and Retention/Expungement Schedules

- **Student Cumulative Records**: Records destroyed one (1) year after separation and transfer to state archives for permanent retention is complete- destruction of these records **is not** permitted
- **Student/Employee Injury Reports**: Records destroyed after seven (7) years; state-archived for six years, then destroyed thereafter
- **Elementary/Middle School Non-transferred Student Files**: Records are destroyed three (3) years after student separation from the district
- **Student Official Transcripts**: Retain for 10 years, then transfer to state archives for permanent retention- destruction of these records **is not** permitted
- **Student Class Attendance Rolls**: Retain for five (5) years, then transfer to state archives for permanent retention- destruction of these records **is not** permitted
- **Special Education Student Records**: Records destroyed three (3) after separation, following the guidelines outlined as follows:

- Paper: Retain in Office for 3 years after Graduation from High School and then microfilm and destroy provided microfilm has passed inspection.
- Microfilm master: Retain in Archives for 3 years after graduation and then destroy.
- Microfilm duplicate: Retain in Office for 3 years after graduation and then destroy.
- Microfilm duplicate: Retain in Archives for 3 years after graduation and then destroy.

## DATA INCIDENT/BREACH RESPONSE PLAN

### Purpose

Provo City School District is committed to appropriately protecting all information relating to its members and affiliates, as well as protecting its confidential business information (including information relating to its employees, affiliates, and students). To achieve this goal and to minimize the risk of loss, theft, or compromise of business or student-related information, appropriate systems, operating procedures, and policies are in effect and are regularly reviewed and updated.

The purpose of this Data Incident/Breach Response Plan is to provide a well-defined and organized approach for handling actual or potential threats to Provo City School District's business or student information maintained electronically (on computers and/or networks), or maintained physically in any other format. This plan is intended to be a durable, living document that may be amended in order to improve or clarify response processes.

The plan also identifies and describes the roles and responsibilities of the Data Privacy Committee, who will put the plan into action.

### Scope

This response plan is meant to address privacy/security incidents involving any and all Provo City School District data, including data under the control or responsibility of a Business Associate or other third-party.

### Goals of Incident/Breach Response

In the event of a privacy/security incident/breach, the goals of Provo City School District's Data Privacy Committee are to:

1. Investigate the incident internally (in cooperation with law enforcement if necessary);
2. Mitigate potential harm to affected parties;
3. Minimize adverse impact to Provo City School District, its employees, and students in an ethically and legally appropriate manner, to include minimizing reduction in operations, reputational harm, and/or financial harm;
4. Appropriately communicate the incident or loss:

    - To affected parties in a timely manner (as appropriate or as otherwise may be required by law);
    - To regulatory agencies, news media, or other entities (as appropriate or required)
    - To staff (as appropriate or required, especially to senior leadership);
5. Provide guidance or assistance in the development of specific corrective actions (including disciplinary action when appropriate); and
6. Conduct post-incident reviews, training, and education, and provide internal communications in order to minimize potential future incidents

**Defining a Data Privacy/Security Incident**

While the major goals described above are common to all privacy or security incidents/breaches, every privacy or security incident/breach involves different degrees of potential risk and different potential for magnitude of harm to Provo City School District, its employees, and students. For instance, a minor incident may involve a low-risk but inappropriate verbal disclosure of information that is non-sensitive in nature, while a major incident may involve loss or disclosure of sensitive information of multiple affected parties.

For the purposes of this response plan, Incidents vary in impact and risk depending on a number of mitigating factors including the content and quantity of the data involved. It is critically important that PCSD management respond quickly and identify the data classification of the incident. This allows staff to respond accordingly in a timely and thorough manner.

**Data classification shall refer to the following PCSD data categories:**

*Public Data*- Information intended for public and community use or information that can be made public without any negative impact on the PCSD or its customers. Student PII shall never be considered public data unless the data has been defined as Directory Information.

*Confidential/Internal Data*- Information of a more sensitive nature to the business and educational operations of PCSD. This data represents basic intellectual capital, applications, and general knowledge. Access shall be limited to only those people that need to know as part of their role within PCSD. Employee and Educator PII (with the exception of social security numbers, financial information, or other critical information) falls within this classification.

*Highly Confidential Data*- Information that, if breached, causes significant damage to PCSD operations, reputation, and/or business continuity. Access to this information should be highly restricted. Student PII falls into this category of data. Employee or Educator Financial Information, Social Security Numbers, and other critical information also fall into this classification.

**Data Breaches or Incidents Classification:**

**Category one: Events**

An event is “any observable occurrence in a system or network,” such as a server receiving a request for a web page, a user sending an email message, or a firewall blocking an attempt to make a connection. Adverse events are those with a “negative consequence, such as unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.”

**Category two: Security Incidents**
A security or electronic incident is an event that violates PCSD's security policies and procedures. We are defining an incident as a security event that compromises the integrity, confidentiality, or availability of an information asset.
Thus, a security incident is an event — such as a malware attack — that puts sensitive data at risk for unauthorized exposure. This could be any type of data, such as regulated financial, medical, or student non-directory information. It can also be unregulated, yet crucial, information like intellectual property.

**Category three: Privacy Incidents**
A privacy incident is an adverse event that may have happened as a result of violating PCSD's privacy policies and procedures. The privacy incident must pertain to the unauthorized use or disclosure of regulated data, like personally identifiable information, protected health information, or student non directory information.
If the data involved in a security incident is regulated, the security incident is "up-leveled" to a privacy incident. In other words, we could safely say that most electronic privacy incidents are security incidents, but not all security incidents are privacy incidents. Privacy incidents can also originate from non-electronic sources, such as mishandled documents, or verbal or visual disclosure of PII or PHI.

**Category four: Data Breach**
If a privacy incident meets specific legal definitions, per state and/or federal breach laws, then it is considered a data breach. It may also be classified as a Data Breach if the Incident Response Team (IRT) determines it based off of the data affected and the risk involved. *Data breaches require notification to the affected individuals, regulatory agencies, and sometimes credit reporting agencies or the media.
Only a small percentage of privacy incidents should escalate into data breaches if effective reporting and risk-mitigation steps are taken and substantiated using the Security Response Plan (SRP) when responding to the privacy incident. A multi-factor risk assessment should be done following the guidelines in the SRP to avoid the risk of over notification or under notification. Organizations should document their incident risk-assessment, notification decision, and timeline when the incident involves regulated data.

**Incident Response Team Members**
Appropriate members of the Data Privacy Committee will be determined by the nature of the incident, but may include a representative(s) from any/all of the following:

- District Data Privacy Coordinator
- IT Security Officer(s)
- Privacy and Security Analyst
- Legal Representatives (when necessary)
- Provo City School District Senior Administrators
- Risk Management
- Information Technology Department
- Public Relations/Marketing Department

- Ancillary Departments
- Third-party vendors engaged to provide incident response services

**Incident Timeline**

Incidents have a timeline that generally contains an Initial Response phase and a Continuing Response phase. Initial Response begins as soon as an incident is discovered or reported and includes time-sensitive first response actions to limit damage while a more organized response is being planned. Continuing Response includes all activities that are conducted necessary to close an incident case and include investigation, correcting processes, notifying affected individuals, and reporting to regulatory agencies as required by law. Generally, the activities within each phase are ongoing and may occur simultaneously, and there may be some overlap between Immediate response activities and continuing response activities. For instance, Investigation may uncover the need for additional analysis, containment, communication, and activation of additional members of the Incident Response Team.

**Discovery/Reporting**

- Determination that an incident has happened
- Involvement of Area Management
- Involvement of IT Department
- Involvement of Student Services Department

**Immediate Response (0--1 Business Day)**

- Containment
- Opening of Incident Case Files
- Escalation
- Activation of the Data Privacy Committee and/or Alternate Plans

**Continuing Response (0-15+ days)**

- Analysis and Planning
- Investigation
- Mitigation and Correction
- Notification
- Closing of Incident Case File
- Reporting

**Discovery and Reporting of a Privacy or Security Incident/Breach**

Information relating to privacy or security incidents/breaches may be reported or discovered in numerous ways. Some of these are listed below:

1. Students, employees, members of the general public, and/or others may report (or complain of) a privacy or security incident/breach to any member of the Provo City School District workforce to include employees, in all sectors, as well as the PCSD District Office mainline;
2. Employees may report an incident to local supervisors/administrators;
3. Workforce members may submit a report by email using their PCSD email address;
4. Employees may report Security Incidents/Breaches by contacting staff in the Information Technology Department;
5. Employees may report directly to the Data Privacy Coordinator using their PCSD email, in-person, or by phone;
6. The Compliance function may observe an incident (for instance, while a member is conducting a staff training or during walkthroughs designed to detect risks or spot improper use, disclosure, storage, transmittal, or disposal of information);
7. Business Associates and/or Third-Party vendors may notify a department with whom they conduct business, a member of senior or executive administration, or the Data Privacy Coordinator.

**Incidents that should be reported may include but are not be limited to:**

a. Student Privacy Complaints relating to:
   - Student Privacy Rights
   - Improper Communications with students
   - Inappropriate use, access or disclosure of personally identifiable information (PII)

b. Employee-related Privacy Concerns relating to:
   - Inappropriate use, access, or disclosure of personally identifiable information (PII)
   - Inappropriate use, access, or disclosure of confidential (non-employee) information
   - Inappropriate modification, deletion, or destruction of employee information

c. Other Concerns relating to:
   - Loss or deletion of stored data (digital or physical); loss or theft of laptops, handheld devices, portable media storage containing confidential business, or individually identifiable information.

d. Theft or Loss of Provo City School District Computer Equipment, including:
   - Desktop computers,
   - Laptop computers,
   - External hard drives
   - Compact disks/DVDs
   - Phones/Tablets/PDAs,
   - Thumb drives,
   - Equipment that stores student, parent, or employee information, or
   - Any other device or storage media (whether issued by Provo City School District or not) which may contain business records or personal information of any potential compromise of Provo City School District students, staff, or affiliates;

e. Computer/Network Intrusions, Data Losses, or other Compromises, including:
   - The unauthorized access, viewing, copying, forwarding, or removal of electronically stored data; or
   - Any other incidents that result/may result in unauthorized acquisition or release of any potential compromise of electronically stored business, student, or employee information.

f. Data Transmission Incidents, including:
- Inadvertent e-mail releases
- Unsecured data transmission
- Malware intrusions

**Determining that an Incident has Occurred**

The PCSD Data Privacy Coordinator and/or IT Security Officers have final determination as to whether an incident/breach has occurred that requires an incident response according to this Incident/Breach Response Plan. An incident is defined in the section titled "Defining a Privacy/Security Incident/Breach."

If a determination is made that no incident has occurred, responding staff will take appropriate steps to close the response and document the non-incident facts and finding that no incident occurred. This may include communications to staff, students, parents of students, keeping in mind that some findings may be restricted.

**Involving Management, IT Security Officers, and/or Data Privacy Coordinator**

Upon discovery of an incident/breach or receipt of a report that an incident/breach has occurred by any member of the Provo City School District workforce:

1. The receiving or discovering workforce member will perform initial information gathering regarding the incident to report to assist with response activities. In general, workforce members should gather:
   - The name and contact information of the reporting individual (if applicable)
   - The location of the incident
   - The circumstances of the incident to include involved parties
2. The receiving or discovering workforce member will communicate incident information to their site administrator, to the Information Technology Departments, and the PCSD Data Privacy Coordinator, as appropriate to the circumstances by phone, email, or other means. I
3. f the site administrator receives a report, it will immediately notify the Information Technology Department and the PCSD Data Privacy Coordinator as appropriate to the circumstances.
4. Site administrators will communicate with the Information Technology Department and the PCSD Data Privacy Coordinator, (as appropriate to the circumstances) regarding actions to contain an incident, investigate an incident, and mitigate damage to affected individuals and to Provo City School District.
5. The Information Technology Department and the PCSD Data Privacy Coordinator will communicate and collaborate regarding privacy/security incidents/breaches.
6. Compliance may require the completion of an Incident Reporting form to obtain enough information to facilitate response. See **Appendix A – Incident Reporting Form**.

**Timeline Note:** Timeliness in reporting to the IT Security Department and Data Privacy Coordinator is critical to ensure timeframes are compliant with the law. By law, privacy/security breaches are considered "discovered" when any member of Provo City School District's workforce knows of it or *should* have known of it in the exercise of due diligence. This discovery date starts the clock that requires investigation and notification within specified timeframes.

**For instance:**

- A student or an employee calls and leaves a voicemail with a complaint that indicates an incident/ breach has occurred. The voicemail is not checked for 9 days. The date of discovery is that date the voicemail was left, shortening investigation and notification timeframes by 9 days.
- An incident/ breach is reported to a manager on January 1. The manager loses the paper on his desk and comes across it on March 16. The date of discovery is January 1. According to law, the organization would already be past legally mandated timeframes and in violation of FERPA Notification Rule.

**After Hours Emergencies**

Generally, most incidents do not require an immediate response and employees can typically wait until the next business day to report. Employees are expected to use professional judgment to determine whether a known or suspected incident is severe enough to warrant an immediate urgent response. In such cases, the employee should contact the following in this order until able to reach one of the persons listed:

1. Security Official: Chad Duncan/Scott Chandler
2. Student Data Privacy Coordinator: Clint Smith
3. Privacy and Security Analyst: JP Pontius

**Initial Response**

Provo City School District's initial response to an incident can make the difference between a situation that is handled properly and a catastrophe. For instance, if a Security Incident is discovered involving hacking of a Provo City School District system or network, the immediate steps taken to stop unauthorized access and secure data could make a huge difference in the amount of damage that could be inflicted to individuals and to Provo City School District.

Depending on the nature of an incident, its scale, potential impact, risk to the organization, or other factors, Provo City School District staff may respond in a variety of ways to include:

- Containment
- Opening of Incident Case Files
- Analysis and Planning
- Escalation & Activation of the Data Privacy Committee

**Containment**

When an incident/ breach is discovered, appropriate members of the Data Privacy Committee may determine the need to conduct containment activities to stop additional information from being lost or disclosed, or to reduce the number of persons to whom information may reach. Data Privacy Committee members may, over their areas of responsibility or collaboratively, take steps to attempt having lost/stolen/inappropriately disclosed information returned or destroyed. For instance, site administrators may attempt to contain and control an incident by suspending certain activities or locking and securing areas of record storage; Human

Resources may suspend employees as appropriate to prevent compromising behavior; and the Information Technology Department may shut down particular applications or third-party connections, reconfigure firewalls, change computer access codes, or change physical access codes.
The IT Security Officer(s) and Data Privacy Coordinator must still be notified of the incident/breach to insure proper notification, resolution and, follow-up by the appropriate members of the Data Privacy Committee.

If applicable, staff members closest to the incident/breach will determine the extent of the incident/breach by identifying all information (and systems) affected, and take action to stop the exposure. This may include:

- Securing or disconnecting affected systems
- Securing affected records or documentation
- Halting affected educational processes
- Pausing any processes that may rely on exposed information or that may have given rise to the incident (as necessary to prevent further use/exposure/etc.)

This would most typically occur in instances of electronic system intrusion, exposed physical (e.g. student) files or records or similar situations.

If the incident occurred at/by a third-party, the Data Privacy Committee will determine if a legal contract and business associate agreement exists and if so, was it violated. The Data Privacy Coordinator will consult the contract/business associate agreement to review the contract terms and determine the next course of action.

**Cyber-insurance and Breach Response Vendors**
If an active cyber-insurance policy exists or the need is otherwise determined, the Data Privacy Committee may contact contracted third-party vendors (cyber-insurance vendors, others) for breach response services and resources to include forensics, investigation and response consulting, notification and call center services, etc. Though recommended to occur as soon as possible after discovery, this can occur at any point as more information is obtained or the need is otherwise determined.

**Documentation/Opening Incident Case Files**
The Data Privacy Coordinator will document all actions taken regarding an incident to include all steps taken in accordance with this plan. This may be done using Compliance generated forms (see **Appendix B – Investigation Activities Log**) incident logs, or systems designated for this purpose. Compliance will begin to establish this documentation as soon as possible, at which point the incident response will be considered an open case file.

Generally speaking, documentation, at a minimum, needs to provide thorough, complete documentation of an incident that can be used to fulfill reporting requirements to government agencies and to organizational senior administrative leadership, as well as serve as legal documentation in the case of a future legal or regulatory proceeding. This documentation will include notations of analyses, notification, reporting, communication, meetings, and all other actions. All documentation related to privacy/security incidents/breaches must be maintained and kept confidential according to the FERPA Document Retention Policy

**Escalation/Activation of the Incident Response Team and/or Alternate Plans**
As more information is gathered, responsible staff will assess each privacy or security incident/breach to determine appropriate handling. This may involve the development and use of internal procedures by individual departments, in coordination with the IT Security Officer(s) and Data Privacy Coordinator.

Additionally, IT Security Officers and the Data Privacy Coordinator will assess each privacy or security incident/breach to determine which parties should be included in communications.

**Some factors to consider when deciding whether to escalate**:

1. Can the incident cause harm to an individual? To what degree?
2. Will the incident require reporting to affected parties, senior administrators, or government agencies?
3. Would the containment, investigation, correction, or other aspect of the incident benefit from cooperation between two or more departments?
4. Does the incident have the potential to cause financial or reputational harm, disruption of operations, or other adverse consequences to the organization, its employees, and/or students?
5. Have involved parties (for example, a complainant) involved legal counsel or threatened legal action?
6. Does the incident involve a business associate or third-party vendor?

Once analysis determines the need for escalation, the Data Privacy Coordinator will activate the Data Privacy Committee to an extent appropriate to each incident/breach. The Data Privacy Coordinator will provide an initial overview of the situation as it pertains to each Data Privacy Committee member's area of responsibility. For instance, the Coordinator may engage the Legal Council when necessary as legal concerns arise or when invoking Attorney-client privilege may be appropriate. The Data Privacy Coordinator will also identify which Data Privacy Committee members will play an active role in the investigation and communicate with them accordingly.

***Escalation: as scale, risk or impact increases, involvement increases***

| Involved Parties | **Technician** (IT team member, Privacy and Security Analyst), **Management** (Site administrator, etc.) | **Department Management** (Data Privacy Coordinator, Security Officers, IT Director, etc.), **Data Privacy Committee** | **Department Administration** (Data Privacy Coordinator, Security Officers, IT Director, etc.), **Data Privacy Committee**, **Senior/Executive Administration** |
|---|---|---|---|
| | Low | Moderate | High |
| | Impact/Risk to Individuals/Organization<br>Or Complexity/Scale | | |

*Responding workforce members are expected to use professional judgment in determining whether an incident is low, medium, or high on the spectrum of scale, risk, or impact. Generally

speaking, a low priority incident is one which poses no risk to business operations or students' privacy and can be appropriately handled by site administrators. A high priority incident poses clear risk to operations of all or part of the district, while medium priority incidents fall in between. When in doubt, responders should inform the Security Officer(s) and Data Privacy Coordinator, who can then determine whether to include others in the incident response.

**Continuing Response**

Provo City School District must continue to take action on an incident/breach in order to understand what has happened, to reduce potential for damages resulting (both to affected individuals and to the organization), to correct what happened, to prevent future recurrence, to inform parties as appropriate, and to fulfill requirements of law.

To do so, the following steps must be carried out in response to privacy/security incidents:

- Investigation
- Mitigation and Correction
- Notification
- Closing of Incident Case File
- Reporting

**Analysis and Planning**

Upon notification of a real or potential privacy/security incident/breach, the Data Privacy Coordinator or designee will perform a preliminary analysis of the facts and assess the situation to determine the nature and extent of the incident. Such analysis may include contacting the individual who reported the problem.
Analysis will also include research into any potential legal concerns beyond the more familiar federal regulations.

The Data Privacy Coordinator or designee, with guidance as necessary from Data Privacy Committee members, will establish a specific incident response plan to investigate the incident, mitigate the damages associated with the exposure or disclosure of personal information, and communicate as necessary with staff, law enforcement, the media, and others. Timeliness of establishing and carrying out the plan may be critical to the public's image of Provo City School District. As needed, any/all members of the Data Privacy Committee may be involved in carrying out the activities of the Incident/Breach Response Plan. The plan will address the following:

- **Review of initial containment activities**
    1. Communication regarding containment activities taken thus far
    2. Assessing risks to information and systems
    3. Determination of additional containment measures
    4. Determination of the need to inform law enforcement (for instance, it may be appropriate to notify the FBI in cases of identity theft or hacking)

[Approval from Legal Council is required unless the workforce member determines a delay could result in harm to the company or to individuals internal or external to the company]

- **Investigation Planning**
    1. Assignment of and coordination with investigators
    2. Evidence gathering planning
    3. Interview planning

- **Communications/Public Relations Planning**
    1. Assess how an incident and the response to it may affect Provo City School District's reputation and public image, or that of its employees and/or students.
    2. Internal Communications
        - Determine the need to notify administration at one, some, or all Provo City School District's facilities
        - Determine the need to notify all current employees/students, and/or parents of students of the incident or employees/students/parents of the affected facility or department only
        - Determine how employees, students, and/or parents will be notified (email, mail to home, mandatory staff meetings, etc.)
        - Determine who will communicate to the staff
        - Determine material content of the notification
    3. External Communications
        - Determine the need for external communications to covered entity, media (press conference or press release if Covered Entity is required to notify the media), etc.
        - Determine who will represent Provo City School District publicly
        - Determine the material content of the Press Conference and/or Press Release
        - Determine the need to post information regarding the incident/breach to the Provo City School District website

**Investigation**

Thorough investigation and documentation of said investigation is a critical component of incident response. Thorough investigation and documentation must be timely, accurate, and professional, and serves several purposes as listed below.

Purposes of thorough Investigation:

- Shows due diligence in complying with legal and regulatory requirements;
- Provides administration and school board with accurate and detailed information. This is essential to correct processes, contain damage, communicate with staff and with external affected persons, and take other appropriate measures;

- Promotes fair, just, and more objective outcomes in regard to the handling of workforce members and/or students, especially as it pertains to discipline;
- Reduces the chances for mistakes that may occur due to incomplete or incorrect information;
- Provides documentation showing the organization's commitment to the protection of the information it holds, and;
- Provides documentation that may be used in civil or criminal proceedings, even years after an incident occurred

Investigation must be timely to insure the most accurate information and to comply with required timeframes. Even so, internal investigations and gathering of data may take several days or even weeks. In the event that law enforcement is involved, this can stretch into months.

**Investigation may involve:**

- If lost/stolen equipment is recovered, the Information Technology Department and the Data Privacy Coordinator may conduct detailed forensics on the equipment in an attempt to determine if business and/or personal information stored on the equipment was accessed or compromised in any way;
- Involved parties may need to notify local and/or federal law enforcement authorities to assist in further investigation, particularly in cases of lost/stolen equipment. In most cases, Legal and Risk Management should be consulted before law enforcement is contacted;
- If an incident involves a third-party, such as a business associate, the Data Privacy Coordinator must communicate with the third-party to determine who will be responsible for notifying local and/or federal law enforcement authorities;
- The Human Resources Department may assist with interviewing workforce members/students; provide guidance to ensure consistent enforcement of discipline; and take action involving staff and/or students (such as suspending employees/students to prevent further damage), and;
- Complainants, recipients of inappropriately disclosed information, and others may be contacted for questioning or to request return or destruction of information.

**Mitigation and Correction**

Provo City School District has a legal and ethical obligation to mitigate (reduce) any harmful effects that result from privacy and security incidents/breaches. Though this is only legally required if Provo City School District "has actual knowledge of harm," Provo City School District will also take reasonable and appropriate steps to prevent harm from occurring either to individuals or to the Provo City School District organization. Actual privacy or security incidents/breaches may result in negative outcomes for the affected parties several months or years later – Provo City School District must acknowledge and be prepared to handle this risk appropriately.

**Examples of Mitigation**:

- Provo City School District may provide "free" credit report monitoring and other "free" services that may be appropriate to affected individuals for specified period of time;

- Compliance, IT, and others may consult with Risk Management and Legal as necessary to understand full scope of risks and potential damages and ways to mitigate;
- Senior administration may determine need for any legal action to be taken on parties (internal or external) involved in the incident;
- Responsible departments may determine need for termination of third-party contract;
- Provo City School District may contact third-party insurers for services or resources related to any purchased policies (for instance, breach response services provided by a cyber-security policy).

Closely tied to mitigation, Correction should occur after any privacy or security incident/breach in order to prevent future recurrence and to comply with organizational policy.

**Examples of Correction**:

- As appropriate, revise written policies and procedures that may be deficient
- Assess informal/unwritten processes and practices and make changes that correct or improve them
- Follow Human Resources and/or Student Services policy and disciplinary action guidelines to determine need for disciplinary action on any Provo City School District employee or student involved in the incident (Human Resources and or Student Services to be involved)
- Determine the need for additional staff/student training
- Determine the need for increased security (physical or electronic) measures

**Notification**

The Data Privacy Committee will determine what notifications are required and will make those notifications in a timely manner in accordance with federal law, state law, and organizational policy (for instance, the Provo City School District Plan titled, "Data Incident/Breach Response Plan" allocates the responsibility for notification of individuals affected by a privacy breach to its Data Privacy Coordinator.

**The Data Privacy Committee will:**

- Determine the need to notify affected individuals. Both state and federal law may have requirements. Notifications should be timely, and conspicuous. Depending on the nature of the incident, notification information may be communicated to the Provo City School District Board of Education or others in order for those entities to provide notification;
- Determine if any other notifications to regulatory entities are required. For instance, specific states may require notification to the state Attorney General's office in the event a Social Security Number is breached;
- Determine if media notification is required (as required by FERPA and Provo City School District policy in some circumstances; composition and delivery of such notice will be conducted by or with approval of Public Relations);
- Determine the means by which individuals and/or other required parties will be notified. Notifications should be delivered in a manner that will ensure the individual receives it. Appropriate delivery methods include written letter, telephone call, or in some cases, substitute forms of notice (conspicuous posting on the website, notification to

major media) as determined to be appropriate by the PCSD Student Services Department, in conjunction with the legal council, and;
- Determine the material content of communication to affected individuals (portions may be pre-determined for efficiency).

**Closing the Incident Case File**

Before an incident case file can be closed, Provo City School District must have met the goals of incident/breach response. To recap, those goals are to:

1. Investigate the incident internally (in cooperation with law enforcement if necessary);
2. Mitigate potential harm to affected parties;
3. Minimize adverse impact to Provo City School District, its employees, students or affiliates in an ethically and legally appropriate manner, to include minimizing reduction in operations, reputational harm, and/or financial harm;
4. Appropriately communicate the incident or loss:
- To affected parties (including students and/or parents of students) in a timely manner (as appropriate or as otherwise may be required by law);
- To regulatory agencies, the news media, or other entities (as appropriate or required);
- To staff (as appropriate or required);
5. Provide guidance or assistance in the development of specific corrective actions (including disciplinary actions when appropriate), and;
6. Conduct post-incident reviews, training and education, and provide internal communications in order to minimize potential future incidents.

All information relating to the incident and activities to meet these goals will be documented in the incident case file before it can be closed. A closed incident case file will be retained according to the FERPA Document Retention Policy.

**Reporting**

Provo City School District will fulfill all reporting requirements under state and federal law. For instance, FERPA requires affected parties be notified of a breach as soon as possible, depending on the information gathered by the responsible parties investigating the breach.

In the event that a breach involves a large number of individuals, the Data Privacy Committee and Public Relations in particular will prepare for fallout that may occur once the covered entity conducts notification of the media.

Additionally, for the purpose of organizational improvement, information from investigation case files may be used to report to staff and administration of various levels in the form of trainings, reports, or other means. Identifying information (both students and staff), students and/or employee-specific information, and other sensitive information will be redacted as appropriate.

Appendix A –Incident Reporting Form

Appendix B – Investigation Activities Log

Appendix C – Notification to Covered Entity